On derivatives of L-series, p-adic cohomology and ray class groups

Kumon, Asuka

Awarding institution:
King's College London

On derivatives of L-series, p-adic cohomology and ray class groups

Asuka Kumon

Supervised by David Burns

A thesis presented for the degree of

Doctor of Philosophy in Pure Mathematics

June 2017

Abstract

We investigate the explicit Galois structure of ray class groups. We also study consequences of the structural results we obtain concerning the validity (or otherwise) of Leopoldt's Conjecture and the existence of families of congruence relations between the values of Dirichlet L-series at $z = 1$.

Acknowledgements

First and foremost, I would like to thank my supervisor David Burns for his constant support and guidance throughout my PhD. I am extremely grateful for his generosity, patience and wisdom, which have made my time at King's both productive and enjoyable. I would also like to thank Manuel Breuning, who inspired me to study in the field of Number Theory during my undergraduate years.

I am also indebted to my fellow PhD students Kwok-Wing Tsoi, Alice Livingstone Boomla, Yasin Zähringer and Tomasz Kosmala for the many hours of (non-)mathematical discussions. I am particularly grateful to Kwok-Wing for his unfailingly positive spirit and invaluable friendship.

I would like to thank my parents for providing me with the encouragement and financial stability which have made my studies possible.

Finally, I would like to thank Jan Felix for his never-ending support and for always making me smile.

I am grateful for the financial support received through the Engineering and Physical Sciences Research Council and King's College London.

Contents

Chapter 1

Introduction

Let L/K be a finite Galois extension of number fields. Fix an odd prime p and let Σ be a finite set of places of K that contains all archimedean places, all places above p and all places that ramify in L/K. Write M_L^Σ for the maximal abelian pro-p extension of L that is unramified outside Σ.

In this thesis, by a *ray class group* we mean a Galois group of the form

$$A_L^\Sigma := \mathrm{Gal}(M_L^\Sigma/L).$$

This is an infinite pro-p abelian group and, since M_L^Σ is a Galois extension of K, there is a natural 'conjugation' action of $\mathrm{Gal}(L/K)$ on A_L^Σ that gives it a $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-module structure.

Ray class groups play a major role in global class field theory and so their module structure is of much interest and has long been studied in its own right. However, in this thesis we investigate two ways in which the study of this structure can have important consequences.

Firstly, the structure of A_L^Σ is closely related to the validity (or otherwise) of a famous conjecture formulated by H.-W. Leopoldt in 1962. In its original form, it conjectures that certain p-adic regulators for number fields do not vanish (for details see, for example, [38, §5.5]). Leopoldt's Conjecture was proved for all number fields that are abelian extensions of $\mathbb{Q}$ by Brumer in 1967 [6] and has since been the subject of much research.

Aside from Brumer's result there has been, as far as we are aware, no other major progress towards the resolution of Leopoldt's Conjecture. However, there have been many equivalent formulations which, at first sight, appear unrelated to p-adic regulators (a list of some of these equivalent forms can be found, for example, in [33, Theorem 10.3.6]).

In particular, the link between the Galois structure of ray class groups and the validity of Leopoldt's Conjecture has been widely studied in the literature, both in relatively elementary ways such as in Miki and Sato [31] and in more advanced 'Iwasawa-theoretic' ways such as, most recently, in Khare and Wintenberger [26].

Secondly, ray class groups occur as the cohomology modules of complexes that play a key role in the formulation of (a special case of) the leading term conjectures for both p-adic and complex valued 'equivariant' L-series that have been studied in recent years. Examples include the 'generalised Iwasawa main conjecture' of Kato [25] and various equivariant refinements of the 'Tamagawa number conjecture' formulated by Bloch and Kato [2].

In particular, detailed structural information about such groups may be used to extract explicit information and predictions from the very abstract statements of these leading term conjectures.

While we will be focusing on better understanding the Galois structure of ray class groups, we will obtain results that have interesting consequences on both of these important areas.

The approach we adopt is largely motivated by a recent article of Burns and Macias

Castillo [12] and subsequent developments of this due to Burns [9].

In particular, in [12, §5] it is shown that Leopoldt's Conjecture can be interpreted in terms of the 'cohomological triviality' of certain $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-modules that are obtained as natural (torsion-free) quotients of A_L^Σ. This relation is particularly interesting since obtaining useful information about the Galois structure of $\mathbb{Z}_p[G]$-lattices that occur naturally in arithmetic is a notoriously difficult problem.

Even in the apparently 'easier' case of valuation rings (rather than ray class groups), one encounters considerable difficulties obtaining concrete information about the explicit Krull-Schmidt decomposition of the valuation ring of a wildly ramified Galois extension of p-adic fields (see, for example, Rzedowski-Calderón et al. [35] and Elder and Madan [16, 17]).

In addition, even for cyclic groups Γ of p-power order, the category of $\mathbb{Z}_p[\Gamma]$-lattices can be extremely complicated to study. In fact, Heller and Reiner [20] have famously shown that the number of isomorphism classes of indecomposable $\mathbb{Z}_p[\Gamma]$-lattices is infinite unless Γ is cyclic of order p or p^2 and, except in these very special cases, there is still no complete classification of such lattices.

Despite these difficulties, in this thesis we will further develop the approach of Burns and Macias Castillo [12] by showing, firstly, that the validity of Leopoldt's Conjecture can be interpreted in terms of the basic properties of two canonical Yoneda extension classes that we introduce. This general result is given in Chapter 3 and also leads us to much more explicit results in later chapters.

Next, in Chapter 4 we apply the general approach introduced by Burns in [9] to study the Selmer modules of critical motives. In particular, we restrict to the case where $\mathrm{Gal}(L/K)$ is a cyclic group of p-power order and apply a representation-theoretic result of Yakovlev to give a characterisation of the $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-module structure of the quotient $\overline{A_L^\Sigma}$ of A_L^Σ by its torsion subgroup.

In this chapter we characterise the extensions L/K for which $\overline{A_L^\Sigma}$ is a 'permutation module' over $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$. We also include a 'finiteness result' concerning the number of isomorphism classes of indecomposable $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-lattices that can occur as direct summands of $\overline{A_L^\Sigma}$, as the extensions L/K range over an infinite family of extensions in which the $\mathbb{Z}_p$-rank of $\overline{A_L^\Sigma}$ cannot be bounded.

In Chapter 5 we specialise further to consider the two classes of cyclic p-power degree extensions in which a complete classification of the isomorphism classes of indecomposable $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-lattices is known, and use methods motivated by Rzedowski-Calderón et al. [35] and Elder and Madan [16, 17] to try to make the results of Chapter 4 more explicit.

For extensions of degree p there are only three isomorphism classes of indecomposable $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-lattices and we are able to give a complete classification of the structure of $\overline{A_L^\Sigma}$. This result also gives a different proof of an earlier observation of Burns and Macias Castillo from [12]. However, for cyclic extensions of degree p^2, the classification theorem of Heller and Reiner gives $4p+1$ isomorphism classes of indecomposable $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-lattices and we have only partial success in using their result to explicitly describe the Galois structure of $\overline{A_L^\Sigma}$.

In Chapter 6 we generalise to extensions L/K that are not necessarily cyclic but assume both that A_K^Σ is torsion-free and that Leopoldt's Conjecture is valid for K at p (following Movahhedi and Nguyen Quang Do [32], such a number field K is said to be 'p-rational'). Under these hypotheses we use the techniques developed in Chapters 3 and 4 to study the Galois structure of A_L^Σ over any finite Galois extension L of K of p-power degree. In this way we obtain some very explicit structure results and also give a new proof of a result of Miki [31] and of Jaulent and Nguyen Quang Do [24] showing that the above hypotheses on K are actually sufficient to imply that Leopoldt's Conjecture is also valid for L at p (irrespective of the nature of the Galois p-extension L/K).

In the remainder of the thesis we assume that p validates Vandiver's Conjecture (as is the case, by Buhler and Harvey [7], for all primes up to $163,577,856$) and specialise to consider the case where $K = \mathbb{Q}$ and L is a cyclotomic field of p-power conductor. In this case $\mathrm{Gal}(L/K)$ is cyclic and one can take Σ to be the set that consists just of the archimedean place of $\mathbb{Q}$ and the prime p. In addition, one knows that Leopoldt's Conjecture is valid for L (by Brumer) and that the relevant special case of the equivariant Tamagawa number conjecture is valid for the extension $L/\mathbb{Q}$ (by Burns and Flach [11]). By combining all these facts, our methods lead to a complete description of the structure of the $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-module A_L^{Σ}.

In particular, in Chapter 7 we give an explicit description of the torsion subgroup of A_L^{Σ} in terms of the value at $z = 1$ of the equivariant Dedekind Zeta function of $L/\mathbb{Q}$ multiplied by a suitable $\mathcal{L}$-invariant. This result is an analogue for ray class groups of Washington's well-known determination of the explicit Galois structure of the ideal class groups of such fields L.

Finally, in Chapter 8, we explain how results in Chapter 7 are used to derive a new family of congruence relations between the (suitably normalised) values at $z = 1$ of Dirichlet L-series of characters of prime power conductor.

Chapter 2

Notation and preliminaries

Throughout we fix an odd prime p. We write $\mathbb{F}_p$ for the field of cardinality p, $\mathbb{Z}_p$ for the ring of p-adic integers and $\mathbb{Q}_p$ for the field of p-adic rationals.

2.1 Algebra

For any abelian group M we set $M_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} M$ and write $M_p^\wedge$ for its pro-p completion $\varprojlim_n M/p^n M$ (so that $M_p = M_p^\wedge$ if M is finitely generated).

For any natural number n we write $M[n]$ for the subgroup of M comprising those elements that have order dividing n. We write $M_{\rm tor}$ for the union of $M[n]$ over all natural numbers n, set

$$\overline{M} := M/M_{\rm tor}$$

and identify $\overline{M}$ with a sublattice of the vector space $\mathbb{Q} \otimes_{\mathbb{Z}} M$ in the obvious way.

If M is a finitely generated $\mathbb{Z}_p$-module we define its '$\mathbb{Z}_p$-rank' to be

$$\mathrm{rk}_{\mathbb{Z}_p}(M) := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} M)$$

and its 'p-rank' to be

$$\mathrm{rk}_p(M) := \dim_{\mathbb{F}_p}(M/pM).$$

We note that $\mathrm{rk}_p(M) = \dim_{\mathbb{F}_p}(M[p]) + \mathrm{rk}_{\mathbb{Z}_p}(M)$ and that for any exact sequence of finitely generated $\mathbb{Z}_p$-modules $M_1 \xrightarrow{\theta_1} M_2 \xrightarrow{\theta_2} M_3$ one has

$$\mathrm{rk}_p(\mathrm{Im}(\theta_i)) \leq \mathrm{rk}_p(M_2) \leq \mathrm{rk}_p(M_1) + \mathrm{rk}_p(M_3)$$

for both $i = 1$ and $i = 2$.

We often abbreviate the vector space $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} M$ to $\mathbb{Q}_p \cdot M$.

If Γ is a finite group, then a finitely generated $\mathbb{Z}_p[\Gamma]$-module M is said to be a '$\mathbb{Z}_p[\Gamma]$-lattice' if M_{tor} vanishes. Each $\mathbb{Z}_p[\Gamma]$-lattice M can therefore be regarded as a submodule of the space $\mathbb{Q}_p \cdot M$.

2.2 Homological algebra

2.2.1 Complexes

Let R be an associative unital noetherian ring. Then by an 'R-module' we will always mean, unless stated otherwise, a left R-module.

We write $D(R)$ for the derived category of (left) R-modules.

Example 2.2.1. For each R-module M and each integer a we write $M[a]$ for the complex $C^\bullet$ for which one has

$$C^i = \begin{cases} M, & \text{if } i = -a \\ 0, & \text{if } i \neq -a \end{cases}$$

and in which all differentials are zero. In this way R-modules give rise to objects of $D(R)$.

For each complex $C^\bullet$ in $D(R)$, with differential d^i in degree i, and for each integer k, the *truncated* complexes $\tau^{\leq k-1}C^\bullet$ and $\tau^{\geq k}C^\bullet$ are defined as follows:

$$
\begin{tikzcd}
\tau^{\leq k-1}C^\bullet : & {} \arrow[r] & C^{k-2} \arrow[r, "d^{k-2}"] \arrow[d, equal] & C^{k-1} \arrow[r, "d^{k-1}"] \arrow[d, equal] & \mathrm{Im}(d^{k-1}) \arrow[r] \arrow[d, hook] & 0 & \\
C^\bullet : & {} \arrow[r] & C^{k-2} \arrow[r, "d^{k-2}"] & C^{k-1} \arrow[r, "d^{k-1}"] & C^k \arrow[r, "d^k"] \arrow[d, two heads] & C^{k+1} \arrow[r, "d^{k+1}"] \arrow[d, equal] & \dots \\
\tau^{\geq k}C^\bullet : & & & 0 \arrow[r] & C^k/\,\mathrm{Im}(d^{k-1}) \arrow[r, "d^k"] & C^{k+1} \arrow[r, "d^{k+1}"] & \dots
\end{tikzcd}
$$

We recall that these complexes give a natural exact triangle

$$\tau^{\leq k-1}C^\bullet \to C^\bullet \to \tau^{\geq k}C^\bullet \to \tag{2.1}$$

in $D(R)$, and that for each integer i one has

$$H^i(\tau^{\leq k-1}C^\bullet) = \begin{cases} H^i(C^\bullet) & \text{if } i \leq k-1 \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \quad H^i(\tau^{\geq k}C^\bullet) = \begin{cases} H^i(C^\bullet) & \text{if } i \geq k \\ 0 & \text{otherwise.} \end{cases}$$

A complex of R-modules is said to be *perfect* if it is isomorphic in $D(R)$ to a bounded complex of finitely generated projective R-modules. We write $D^{\mathrm{perf}}(R)$ for the full triangulated subcategory of $D(R)$ comprising complexes that are perfect.

Remark 2.2.2. If $C^\bullet$ belongs to $D^{\mathrm{perf}}(R)$, then there can exist integers k for which the truncated complexes $\tau^{\leq k-1}C^\bullet$ and $\tau^{\geq k}C^\bullet$ do not belong to $D^{\mathrm{perf}}(R)$.

2.2.2 Cohomologically trivial modules

In this section we recall two prove two useful results for the special case that $R := \mathbb{Z}_p[G]$ for a finite group G.

Recall that a $\mathbb{Z}_p[G]$-module M is said to be *cohomologically trivial* if for all subgroups J of G and all integers i the Tate cohomology group $\hat{H}^i(J, M)$ vanishes.

The first result interprets this notion in terms of the notion of perfect complexes.

Lemma 2.2.3. Set $R := \mathbb{Z}_p[G]$ for a finite group G. Let a be an integer and M a finitely generated R-module. Then $M[-a]$ belongs to $D^{\mathrm{perf}}(R)$ if and only if M is a cohomologically trivial G-module.

Proof. Since M is a finitely generated R-module, a standard argument implies that $M[-a]$ is isomorphic to a complex $P^\bullet$ of finitely generated projective R-modules with the property that $P^b = 0$ for all $b > a$. This means that there is an exact sequence of R-modules of the form

$$\cdots \to P^c \xrightarrow{d^c} P^{c+1} \xrightarrow{d^{c+1}} \cdots \xrightarrow{d^{a-1}} P^a \to M \to 0.$$

Now since $M[-a]$ belongs to $D^{\mathrm{perf}}(R)$ if and only if there exists such a complex $P^\bullet$ that is bounded (i.e. such that $P^c = 0$ for all sufficiently small c), this exact sequence implies that $M[-a]$ belongs to $D^{\mathrm{perf}}(R)$ if and only if the R-module M has finite projective dimension.

Therefore it is enough to recall that the argument of [5, Chapter VI, Theorem 8.12] implies that a finitely generated $\mathbb{Z}_p[G]$-module has finite projective dimension if and only if it is a cohomologically trivial G-module. $\square$

The next result gives a lower bound on the cardinality of any non-zero finite cohomologically trivial G-module.

We believe that this result is essentially well-known but for completeness we give a proof (indicated by my research supervisor).

Lemma 2.2.4. Let P be a finite abelian group of p-power order and write Δ_P for the number of orbits of the natural action of $\mathrm{Gal}(\mathbb{Q}_p^c\,/\,\mathbb{Q}_p)$ on $P^* := \mathrm{Hom}(P, \mathbb{Q}_p^{c\times})$. Then any non-trivial finite abelian group of p-power order that is a cohomologically trivial P-module has order divisible by p^{Δ_P}.

Proof. Set $R := \mathbb{Z}_p[P]$. Then R is a local ring and hence if M is a finite abelian group of p-power order of the stated kind, then the argument used above shows there exists an exact sequence of finitely generated R-modules of the form

$$0 \to N \xrightarrow{\theta} N \to M \to 0 \tag{2.2}$$

where N is free. This sequence implies that $|M| = |\,\mathbb{Z}_p\,/(d_\theta)|$ with $d_\theta := \det_{\mathbb{Z}_p}(\theta)$.

To compute d_θ we write r for the rank of N and represent θ by a matrix Θ in $\mathrm{M}_r(R) \cap \mathrm{GL}_r(\mathbb{Q}_p[P])$. Then $d_\theta = \prod_{\chi \in P^*} d_\theta(\chi)$ with $d_\theta(\chi) := \det(\Theta_\chi)$ where Θ_χ is the matrix in $\mathrm{M}_r(\mathbb{Z}_p[\chi])$ obtained by applying the $\mathbb{Z}_p$-linear extension $R \to \mathbb{Z}_p[\chi]$ of χ to each entry of Θ. In particular, since $d_\theta(\omega \circ \chi) = \omega(d_\theta(\chi))$ for each $\chi \in P^*$ and $\omega \in \mathrm{Gal}(\mathbb{Q}_p^c\,/\,\mathbb{Q}_p)$, one has

$$d_\theta = \prod_{\chi \in \Upsilon} \mathrm{N}_{\mathbb{Q}_p(\chi)/\mathbb{Q}_p}(d_\theta(\chi)) \tag{2.3}$$

where Υ is a set of representatives of the orbits of the action of $\mathrm{Gal}(\mathbb{Q}_p^c\,/\,\mathbb{Q}_p)$ on P^*.

Taking P-coinvariants of (2.2) we obtain an exact sequence of $\mathbb{Z}_p$-modules

$$0 \to H_0(P, N) \xrightarrow{H_0(P,\theta)} H_0(P, N) \to H_0(P, M) \to 0$$

and, since $H_0(P, M)$ is non-zero, this sequence implies that $d_\theta(\mathbf{1}_P)$ belongs to the ideal (p) of $\mathbb{Z}_p$.

In addition, if for each $\chi \in \Upsilon$ we write $\mathfrak{p}_\chi$ for the maximal ideal of $\mathbb{Z}_p[\chi]$, then one has

$$d_\theta(\chi) \equiv d_\theta(\mathbf{1}_P) \text{ (modulo } \mathfrak{p}_\chi).$$

This implies that $d_\theta(\chi)$ belongs to $\mathfrak{p}_\chi$ and hence that $\mathrm{N}_{\mathbb{Q}_p(\chi)/\mathbb{Q}_p}(d_\theta(\chi))$ belongs to (p).

These observations combine with (2.3) to imply d_θ belongs to $(p)^{|\Upsilon|}$ and hence that $|M|$ is divisible by $p^{|\Upsilon|} = p^{\Delta_P}$, as claimed. □

2.2.3 Determinants and Fitting ideals

In this section we recall the relevant details of the 'determinant functor' of Knudsen and Mumford [28] in the setting of objects of $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$ for a finite abelian group G.

Since $\mathbb{Z}_p[G]$ is a finite direct product of commutative local rings we can replace $\mathbb{Z}_p[G]$ by a local component R (and then deal with the general case as the 'direct sum' of the cases for each local component).

An R-module is projective if and only if it is free and so each complex in $D^{\mathrm{perf}}(R)$ is isomorphic to a bounded complex of finitely generated free R-modules.

If M is a free R-module of rank d, then we define its *determinant* by setting

$$\mathrm{Det}_R(M) := (\bigwedge\nolimits_R^d M, d),$$

where $\bigwedge_R^d$ denotes the d-th exterior power of R-modules and the pair $(-,-)$ is regarded as a 'graded invertible' R-module, and also set

$$\mathrm{Det}_R(M)^{-1} := (\mathrm{Hom}_R(\bigwedge\nolimits_R^d M, R), -d).$$

For two such modules (M_1, d_1) and (M_2, d_2) we set

$$(M_1, d_1) \otimes (M_2, d_2) := (M_1 \otimes_R M_2, d_1 + d_2)$$

which is again a graded invertible module.

In particular, there is a natural 'evaluation pairing' isomorphism

$$\mathrm{Det}_R(M) \otimes \mathrm{Det}_R(M)^{-1} \cong (R, 0) \tag{2.4}$$

induced by sending $x \otimes \phi$ to $\phi(x)$ for each x in $\bigwedge_R^d M$ and ϕ in $\mathrm{Hom}_R(\bigwedge_R^d M, R)$.

We now consider a short exact sequence of finitely generated, free R-modules

$$0 \to M_1 \to M_2 \xrightarrow{\theta} M_3 \to 0$$

and fix an R-basis $\{b_j^i : 1 \leq j \leq d_i\}$ for each module M_i.

Since θ is surjective we can choose for j with $1 \leq j \leq d_3$ an element $\hat{b}_j^3$ of M_2 with $\theta(\hat{b}_j^3) = b_j^3$. Then $\{b_j^1 : 1 \leq j \leq d_1\} \cup \{\hat{b}_j^3 : 1 \leq j \leq d_3\}$ is an R-basis of M_2 and there is an isomorphism of graded R-modules

$$\mathrm{Det}_R(M_2) \cong \mathrm{Det}_R(M_1) \otimes \mathrm{Det}_R(M_3) \tag{2.5}$$

that is induced by sending the basis $(\bigwedge_{i=1}^{i=d_1} b_i^1) \wedge (\bigwedge_{j=1}^{j=d_3} \hat{b}_j^3)$ of $\bigwedge_R^{d_2} M_2$ to $(\bigwedge_{i=1}^{i=d_1} b_i^1) \otimes (\bigwedge_{j=1}^{j=d_3} b_j^3)$.

Remark 2.2.5. The grading is used by Knudsen and Mumford to avoid certain 'sign problems' that can arise in isomorphisms of the form (2.5). However, this does not play a major role in our work and so we sometimes do not mention it explicitly, and therefore identify $\mathrm{Det}_R(M)$ with the free rank one R-module $\bigwedge_R^d M$.

Now, if $C^\bullet$ is a complex in $D^{\mathrm{perf}}(R)$ represented by a bounded complex of finitely generated free R-modules

$$0 \to \cdots \xrightarrow{d^{a-1}} M^a \xrightarrow{d^a} M^{a+1} \xrightarrow{d^{a+1}} \cdots \to 0, \tag{2.6}$$

then its *determinant module* is defined by setting

$$\mathrm{Det}_R(C^\bullet) := \bigotimes_{a\in\mathbb{Z}} \mathrm{Det}_R(M^a)^{(-1)^a}$$

where the tensor product is of graded R-modules.

Knudsen and Mumford show that this definition depends only on the isomorphism class of $C^\bullet$ in $D^{\mathrm{perf}}(R)$. In addition, for any exact triangle in $D^{\mathrm{perf}}(R)$ of the form $C_1^\bullet \to C_2^\bullet \to C_3^\bullet \to$ the construction of (2.5) extends to give a natural isomorphism of graded modules

$$\mathrm{Det}_R(C_2^\bullet) \cong \mathrm{Det}_R(C_1^\bullet) \otimes \mathrm{Det}_R(C_3^\bullet). \tag{2.7}$$

We now fix an extension E of $\mathbb{Q}_p$ and for each R-module M set $M_E := E \otimes_{\mathbb{Z}_p} M$. We note that R_E is a finite product of fields and hence that all of the constructions made above extend to the setting of R_E modules.

We also fix a complex $C^\bullet$ in $D^{\mathrm{perf}}(R)$ and a representative of $C^\bullet$ of the form (2.6). Then in each degree i there are exact sequences of projective R_E-modules

$$0 \to \mathrm{Im}(d^{i-1})_E \to \ker(d^i)_E \to H^i(C^\bullet)_E \to 0 \tag{2.8}$$

$$0 \to \ker(d^i)_E \to M_E^i \to \mathrm{Im}(d^i)_E \to 0. \tag{2.9}$$

The isomorphism (2.5) combines with the above exact sequences to give a composite 'passage to cohomology' isomorphism

$$\begin{aligned}\mathrm{Det}_R(C^\bullet)_E &= \bigotimes_{i\in\mathbb{Z}} \mathrm{Det}_{R_E}(M^i_E)^{(-1)^i}\\ &\cong \bigotimes_{i\in\mathbb{Z}} [\mathrm{Det}_{R_E}(\ker(d^i)_E) \otimes \mathrm{Det}_{R_E}(\mathrm{Im}(d^i)_E)]^{(-1)^i}\\ &\cong \bigotimes_{i\in\mathbb{Z}} (\mathrm{Det}_{R_E}(H^i(C^\bullet)_E))^{(-1)^i}.\end{aligned}$$

where the first isomorphism comes from (2.9) and the second from (2.8).

We now assume that $H^a(C^\bullet) = 0$ for all $a \notin \{i, i+1\}$ for some integer i and that there exists an isomorphism of R_E-modules $\mu : H^i(C^\bullet)_E \cong H^{i+1}(C^\bullet)_E$.

In such a case we write ϑ_μ for the composite isomorphism

$$\begin{aligned}\mathrm{Det}_R(C^\bullet)_E &\cong \mathrm{Det}_{R_E}(H^i(C^\bullet)_E)^{(-1)^i} \otimes \mathrm{Det}_{R_E}(H^{i+1}(C^\bullet))^{(-1)^{i+1}}\\ &\cong \mathrm{Det}_{R_E}(H^{i+1}(C^\bullet)_E)^{(-1)^i} \otimes \mathrm{Det}_{R_E}(H^{i+1}(C^\bullet)_E)^{(-1)^{i+1}}\\ &\cong (R_E, 0)\end{aligned}$$

where the first map is the 'passage to cohomology' isomorphism, the second is $\mathrm{Det}_{R_E}(\mu)^{(-1)^i} \otimes \mathrm{id}$ and the third is the appropriate case of (2.4).

The free rank one R-submodule $\Xi(C^\bullet, \mu)$ of R_E that is specified by the equality

$$\vartheta_\mu(\mathrm{Det}_R(C^\bullet)) = (\Xi(C^\bullet, \mu), 0)$$

depends only on $C^\bullet$ and μ and will play an important role in later chapters.

Remark 2.2.6. Let G be a finite abelian group, M a finite cohomologically trivial G-module and a an integer. Then Lemma 2.2.3 implies that $M[-a]$ belongs to $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$. In addition, since the module $H^a(M[-a])_{\mathbb{Q}_p} = M_{\mathbb{Q}_p}$ vanishes one can apply the above construction with

$E = \mathbb{Q}_p$ and μ the zero map.

In this case we also know that, for any sufficiently large integer b, there exists an exact sequence of $\mathbb{Z}_p[G]$-modules of the form

$$0 \to \mathbb{Z}_p[G]^b \xrightarrow{\kappa} \mathbb{Z}_p[G]^b \to M \to 0$$

and, by using this, one computes that $\Xi(M[-a], 0)$ is equal to

$$(\mathbb{Z}_p[G] \cdot \det(\kappa)^{(-1)^{a-1}}, 0) = (\mathrm{Fit}_{\mathbb{Z}_p[G]}(M)^{(-1)^{a-1}}, 0),$$

where $\mathrm{Fit}_{\mathbb{Z}_p[G]}(M)$ denotes the zeroth Fitting ideal of M and is an invertible ideal of $\mathbb{Z}_p[G]$.

Remark 2.2.7. The standard reference for Fitting ideals is Northcott's book [34]. In the case where M is a cyclic R-module, $\mathrm{Fit}_R(M)$ is equal to the annihilator ideal of M in R and hence M is isomorphic to $R/\mathrm{Fit}_R(M)$.

2.2.4 Yoneda extensions

Let R be an associative unital noetherian ring and let M and N be R-modules. For each natural number n one defines a 'Yoneda n-extension of M by N' to be an exact sequence of R-modules of the form

$$E : 0 \to N \to E_n \to \cdots \to E_1 \to M \to 0.$$

We say that any two such extensions E and E' satisfy the relation '$E \sim E'$' if there is a commutative diagram of the form

$$\begin{array}{ccccccccccccc} E : 0 & \longrightarrow & N & \longrightarrow & E_n & \longrightarrow & \dots & \longrightarrow & E_1 & \longrightarrow & M & \longrightarrow & 0 \\ & & \| & & \downarrow & & & & \downarrow & & \| & & \\ E' : 0 & \longrightarrow & N & \longrightarrow & E'_n & \longrightarrow & \dots & \longrightarrow & E'_1 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

or a similar diagram with the vertical arrows reversed. We then say that two n-extensions E and E' are 'equivalent' if there exists a finite chain $E = E_1, E_2, \dots, E_k = E'$ of n-extensions with the property that $E_1 \sim E_1 \sim \dots \sim E_k$.

It can be shown that this relation is an equivalence relation, that the set $\mathrm{YExt}^n_G(M, N)$ of equivalence classes has an abelian group structure and that this group is canonically isomorphic to the derived-functor Ext-group $\mathrm{Ext}^n_R(M, N)$ (see, for example, [23, Theorem 9.1]).

Remark 2.2.8. In particular, if $R = \mathbb{Z}_p[G]$ and $M = \mathbb{Z}_p$, then the group $\mathrm{YExt}^1_R(M, N)$ is isomorphic to the cohomology group $H^i(G, N)$.

Example 2.2.9. For any ring R as above, the *split one-extension* of M by N is the natural short exact sequence $0 \to N \to N \oplus M \to M \to 0$ and corresponds to the trivial element of $\mathrm{YExt}^1_G(M, N)$.

2.3 Arithmetic

2.3.1 Fields and groups

We fix an algebraic closure $\mathbb{Q}^c$ of $\mathbb{Q}$ and for each number field L in $\mathbb{Q}^c$ we set $G_L := \mathrm{Gal}(\mathbb{Q}^c/L)$. We also write L^{cyc} for the cyclotomic $\mathbb{Z}_p$-extension of a number field L and set $\Gamma_L := \mathrm{Gal}(L^{\mathrm{cyc}}/L)$.

For any finite set of places Σ of L containing all archimedean places and all places above p we write M_L^Σ for the maximal abelian pro-p extension of L in $\mathbb{Q}^c$ that is unramified outside all places in Σ. We observe that M_L^Σ contains L^{cyc} and set $A_L^\Sigma := \mathrm{Gal}(M_L^\Sigma/L)$ and $B_L^\Sigma := \mathrm{Gal}(M_L^\Sigma/L^{\mathrm{cyc}})$. This can be shown on the field diagram:

$$\begin{tikzcd}[arrows=dash]
M_L^\Sigma \arrow[dd, "A_L^\Sigma"'] \arrow[dr, "B_L^\Sigma"] & \\
 & L^{\mathrm{cyc}} \arrow[dl, "\Gamma_L"] \\
L &
\end{tikzcd}$$

In the case that Σ just comprises all places that are either archimedean or p-adic, then we often abbreviate A_L^Σ and B_L^Σ to A_L^p and B_L^p respectively.

We now assume that L is a finite Galois extension of K with $G := \mathrm{Gal}(L/K)$, and that Σ comes from the set of places of L that lie above a given set of places Σ' of K. In this case we often write $A_L^{\Sigma'}$ and $B_L^{\Sigma'}$ in place of A_L^Σ and B_L^Σ

Under these hypotheses, the field M_L^Σ is a Galois extension of K and each of the groups A_L^Σ, B_L^Σ and Γ_L can be regarded as $\mathbb{Z}_p[G]$-modules via the natural conjugation action of G as follows: for each $g \in G$ and $\sigma \in A_L^\Sigma$ we set

$$g \cdot \sigma := \tilde{g} \cdot \sigma \cdot \tilde{g}^{-1}$$

where $\tilde{g}$ is any lift of g to an element of $\mathrm{Gal}(M_L^\Sigma/K)$. This definition is independent of the choice of lift $\tilde{g}$ and, with respect to this action, the group B_L^Σ is a $\mathbb{Z}_p[G]$-submodule of A_L^Σ and the induced action of G on the quotient group $A_L^\Sigma/B_L^\Sigma \cong \Gamma_L$ is trivial.

2.3.2 Galois cohomology

We write $\mathcal{O}_{L,\Sigma}$ for the subring of L comprising elements of L which are integral at all places outside those which lie above a place in Σ. Let L_Σ be the maximum algebraic extension of L

in $\mathbb{Q}^c$ unramified outside Σ, and write $G_{L,\Sigma}$ for $\mathrm{Gal}(L_\Sigma/L)$.

Define $\mathbb{Z}_p(1)$ to be the inverse limit $\varprojlim \mu_{p^n}$ of the groups of p^n-th roots of unity in $\mathbb{Q}^c$, and note that this is a continuous $\mathbb{Z}_p[G_{L,\Sigma}]$-module. Writing w_v for a place in L_Σ which lies above a $v \in \Sigma$ and $\mathcal{G}_{w_v}$ for the corresponding decomposition group, there is a 'localisation' morphism

$$C^\bullet(G_{L,\Sigma}, \mathbb{Z}_p(1)) \to \bigoplus_{v\in\Sigma} C^\bullet(\mathcal{G}_{w_v}, \mathbb{Z}_p(1)).$$

Define $R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ to be the mapping fibre of this morphism, giving an exact triangle

$$R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1)) \to C^\bullet(G_{L,\Sigma}, \mathbb{Z}_p(1)) \to \bigoplus_{v\in\Sigma} C^\bullet(\mathcal{G}_{w_v}, \mathbb{Z}_p(1)).$$

The basic properties of this complex are well-known and are, for convenience, recalled in the next result.

In this result we write Σ_L for the set of all complex embeddings $L \to \mathbb{C}$ and consider the direct sum

$$W'_L := \bigoplus_{\Sigma_L} 2\pi i \cdot \mathbb{Z}$$

as a $G \times \mathrm{Gal}(\mathbb{C}/\mathbb{R})$-module, where G acts on Σ_L via pre-composition and $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts diagonally (via post-composition on Σ_L).

We then obtain a $\mathbb{Z}_p[G]$-module by setting $W_{L,p} := H^0(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), W'_L)_p$.

Proposition 2.3.1. Set $C^\bullet := R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$.

(i) $C^\bullet$ belongs to $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$.

(ii) $C^\bullet$ is acyclic outside degrees 1, 2 and 3.

(iii) There are identifications $H^2(C^\bullet) = A_L^\Sigma$ and $H^3(C^\bullet) = \mathbb{Z}_p$ and a natural exact sequence

$$0 \to W_{L,p} \to H^1(C^\bullet) \to \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_L^\times \xrightarrow{\lambda_{L,p}} \bigoplus_w (\mathcal{O}_{L_w}^\times)_p^\wedge$$

where in the direct sum w runs over all places of L above p, $\mathcal{O}_{L_w}$ denotes the valuation ring of L_w and $\lambda_{L,p}$ is the natural diagonal localisation map.

(iv) The $\mathbb{Q}_p[G]$-modules $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2(C^\bullet)$ and $(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(C^\bullet)) \oplus (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^3(C^\bullet))$ are isomorphic.

Proof. Since Σ is assumed to contain all places that ramify in L/K, claim (i) is a standard property of étale cohomology which is proved by Flach in [18, Theorem 5.1].

The explicit descriptions in claims (ii) and (iii) are obtained, for example, in the course of the proof given by Castillo and Jones of [13, Proposition 2.1].

Since the algebra $\mathbb{Q}_p[G]$ is semisimple, claim (iv) follows from the general property of étale cohomology complexes proved in [10, Lemma 7]. $\square$

Chapter 3

Leopoldt's Conjecture and canonical extension classes

In this chapter we give a new interpretation of the validity (or otherwise) of Leopoldt's Conjecture in terms of the properties of certain Yoneda extension classes.

The results described here both complement and extend those recently obtained by Burns and Macias Castillo in [12, §5].

In addition, they will play an important part in later chapters when we obtain explicit descriptions of the Galois structure of ray class groups and also establish new families of congruences between the values at $s = 1$ of Dirichlet L-series.

The results of this section were obtained in collaborative work with my research supervisor.

3.1 The cyclotomic and étale extension classes

We fix a finite Galois extension of number fields L/K and set $G := \mathrm{Gal}(L/K)$. We also fix a finite set of places Σ of K that contains all archimedean places, all places above p and all places that ramify in L/K.

3.1.1 The cyclotomic extension class

We fix a topological generator γ_L of $\Gamma_L = \mathrm{Gal}(L^{\mathrm{cyc}}/L)$ and use it to identify Γ_L with $\mathbb{Z}_p$ by the map sending γ_L to 1. Then the tautological short exact sequence of $\mathbb{Z}_p[G]$-modules

$$0 \to B_L^{\Sigma} \to A_L^{\Sigma} \to \Gamma_L \to 0 \tag{3.1}$$

gives rise to an element $c_{L/K}^{\Sigma,\gamma_L}$ of the group

$$\mathrm{YExt}^1_G(\Gamma_L, B_L^{\Sigma}) = \mathrm{YExt}^1_G(\mathbb{Z}_p, B_L^{\Sigma}) \cong H^1(G, B_L^{\Sigma}) \tag{3.2}$$

where the equality depends on the choice of γ_L and the isomorphism is from Remark 2.2.8.

Definition 3.1.1. We define the *cyclotomic extension class* $c_{L/K}^{\Sigma,\gamma_L}$ associated to the extension L/K, the set Σ and the element γ_L to be the element of $H^1(G, B_L^{\Sigma})$ that corresponds under the isomorphism (3.2) to the extension (3.1).

3.1.2 The étale extension class

We now use the compactly supported étale cohomology complex $C^\bullet = R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ that is described in Proposition 2.3.1.

The truncated complex $\tau^{\geq 2}C^\bullet$ is acyclic outside degrees two and three and there are identifications $H^2(\tau^{\geq 2}C^\bullet) = A_L^{\Sigma}$ and $H^3(\tau^{\geq 2}C^\bullet) = \mathbb{Z}_p$.

This implies that one can choose an exact sequence of $\mathbb{Z}_p[G]$-modules

$$0 \to A_L^{\Sigma} \to D^2 \xrightarrow{d} D^3 \to \mathbb{Z}_p \to 0 \tag{3.3}$$

with the following property: if one writes $D^\bullet$ for the complex $D^2 \xrightarrow{d} D^3$, where the first term is placed in degree two, and uses the maps in the above sequence to identify $H^2(D^\bullet) = \ker(d)$

and $H^3(D^\bullet) = \mathrm{cok}(d)$ with A_L^Σ and $\mathbb{Z}_p$, then there exists an isomorphism θ in $D(\mathbb{Z}_p[G])$ between $\tau^{\geq 2}C^\bullet$ and $D^\bullet$ such that $H^2(\theta)$ and $H^3(\theta)$ are the identity maps on A_L^Σ and $\mathbb{Z}_p$ respectively.

It is not difficult to show that the element $\tilde{c}_{L/K}^{\Sigma,\text{ét}}$ of $\mathrm{YExt}_G^2(\mathbb{Z}_p, A_L^\Sigma)$ that corresponds to (3.3) depends only on the complex $\tau^{\geq 2}C^\bullet$, rather than on the precise choice of extension (3.3) with the above properties (see, for example, the discussion given in [8, §3.1]).

Definition 3.1.2. We define the *étale extension class* associated to the data L/K and Σ to be the image $c_{L/K}^{\Sigma,\text{ét}}$ in $H^2(G, A_L^\Sigma)$ of the Yoneda extension $\tilde{c}_{L/K}^{\Sigma,\text{ét}}$ under the natural isomorphism $\mathrm{YExt}_G^2(\mathbb{Z}_p, A_L^\Sigma) \cong H^2(G, A_L^\Sigma)$.

3.2 Statement of the main results

In this section we state the main results of this chapter.

This first result gives a new interpretation of Leopoldt's Conjecture in terms of the canonical extension classes defined above:

Theorem 3.2.1. The following conditions are equivalent.

(i) Leopoldt's Conjecture is valid at p.

(ii) For all finite Galois extensions of number fields L/K, with $G = \mathrm{Gal}(L/K)$, and all finite sets of places Σ of K that contain all archimedean places, p-adic places and all those that ramify in L/K, the complex $\tau^{\geq 2}R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ belongs to $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$.

(iii) For all L/K and Σ as in claim (ii) one has both

   (a) $c_{L/K}^{\Sigma,\gamma_L}$ generates $H^1(G, B_L^\Sigma)$, and

   (b) $c_{L/K}^{\Sigma,\text{ét}}$ generates $H^2(G, A_L^\Sigma)$ and has order $|G|$.

Remark 3.2.2. The proof of Theorem 3.2.1 that we give below actually shows that claim (iii) is equivalent to saying that the G-module A_L^Σ is a class module with fundamental class $c_{L/K}^{\Sigma,\text{ét}}$ (as defined, for example, in [33, Chapter III, Definition (3.1.3)]). This statement is a p-adic analogue of the classical fact that the Σ-idele class group of L is a class module for G.

We will also show that Theorem 3.2.1 has the following consequence regarding cyclotomic extension classes and hence the Galois structure of ray class groups.

Corollary 3.2.3. Let L/K be a finite Galois extension of number fields with Galois group G, and Σ a finite set of places of K that contains all archimedean places, places above p and all those that ramify in L/K. If L validates Leopoldt's Conjecture at p, then the following conditions are equivalent.

(i) $c_{L/K}^{\Sigma,\gamma_L}$ vanishes (and so the canonical extension (3.1) splits).

(ii) The G-module B_L^Σ is cohomologically trivial.

(iii) Let P be a Sylow p-subgroup of G and set $F := L^P$. Then one of the following conditions is satisfied:

  (a) L is contained in F^{cyc};

  (b) L is disjoint from F^{cyc}, P is cyclic and for each non-trivial subgroup C of P, with $E := L^C$, the maximal abelian extension of E^{cyc} in M_L^Σ is equal to M_E^Σ and the transfer map from $A_E^\Sigma := \mathrm{Gal}(M_E^\Sigma/E) = \mathrm{Gal}(M_L^\Sigma/E)^{\text{ab}}$ to $\mathrm{Gal}(M_L^\Sigma/L)^{\text{ab}} = \mathrm{Gal}(M_L^\Sigma/L) =: A_L^\Sigma$ is injective upon restriction to the torsion subgroup of $\mathrm{Gal}(M_E^\Sigma/L^{\text{cyc}})$.

We end this section by giving a direct proof that, without any hypothesis on Leopoldt's Conjecture, the element $c_{L/K}^{\Sigma,\gamma_L}$ vanishes for any proper subfield of K^{cyc}. This case plays an important part in later sections.

Corollary 3.2.4. Let K be a number field and L a proper subfield of the cyclotomic $\mathbb{Z}_p$-extension K^{cyc} of K. Then for any finite set of places Σ of K that contains all archimedean places, places above p and all those that ramify in L/K, the cyclotomic extension class $c_{L/K}^{\Sigma,\gamma_L}$ vanishes. In particular, in this case the validity of Leopoldt's Conjecture at p implies that the equivalent conditions of Corollary 3.2.3 (i), (ii) and (iii) are satisfied.

Proof. Let L be a proper subfield of K^{cyc}, with $[L:K]=p^n$, and Σ a finite set of places as above.

Fix an element γ of $\mathrm{Gal}(M_L^\Sigma/K)$ that projects to give a topological generator of Γ_K and hence also projects to give a generator of $G := \mathrm{Gal}(L/K)$.

Then the element γ^{p^n} belongs to $\mathrm{Gal}(M_L^\Sigma/L) = A_L^\Sigma$ and also projects to give a topological generator γ' of $\Gamma_L = \Gamma_K^{p^n}$.

In addition, any element x of $\mathrm{Gal}(M_L^\Sigma/K)$ can be written as $x = a\cdot\gamma^i$ with a an element of A_L^Σ and i an integer and so

$$\gamma^{p^n}\cdot x = \gamma^{p^n}\cdot(a\gamma^i) = a\gamma^{p^n}\gamma^i = (a\gamma^i)\cdot\gamma^{p^n}$$

where the second equality is true because both a and γ^{p^n} belong to the abelian group A_L^Σ.

This shows that the γ^{p^n} belongs to the centre of $\mathrm{Gal}(M_L^\Sigma/K)$ and hence the conjugation action of G on γ^{p^n} is trivial. Therefore the unique homomorphism of $\mathbb{Z}_p$-modules $\Gamma_L \to A_L^\Sigma$ that sends γ' to γ^{p^n} is a homomorphism of $\mathbb{Z}_p[G]$-modules that splits the tautological extension (3.1) in this case.

It follows that the element $c_{L/K}^{\Sigma,\gamma_L}$ vanishes and then the claimed result is a direct consequence of Corollary 3.2.3. $\square$

3.3 Preliminary observations

We start by using Proposition 2.3.1 to derive conditions that are equivalent to the validity of Leopoldt's Conjecture.

We recall that we write r_E for the number of complex places of a number field E.

Proposition 3.3.1. Let L/K be a finite Galois extension of number fields and set $G := \mathrm{Gal}(L/K)$. Let Σ be a finite set of places of K containing all archimedean places, places above p and all those that ramify in L/K.

(i) The following conditions are equivalent.

- (a) Leopoldt's Conjecture is valid for L at p.
- (b) $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$ identifies with $W_{L,p}$.
- (c) The $\mathbb{Q}_p[G]$-modules $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_L^\Sigma$ and $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} W_{L,p}$ are isomorphic.

(ii) If no archimedean place of K ramifies in L, then the following conditions are equivalent.

- (a) Leopoldt's Conjecture is valid for L at p.
- (b) Leopoldt's Conjecture is valid for K at p and B_L^Σ spans a free $\mathbb{Q}_p[G]$-module.
- (c) B_L^Σ spans a free $\mathbb{Q}_p[G]$-module of rank r_K.

Proof. If Leopoldt's Conjecture is valid for L at p, then the homomorphism $\lambda_{L,p}$ in Proposition 2.3.1(iii) is injective (by [33, Theorem 10.3.6 (iii)]). Given this, the equivalence of conditions (i)(a) and (i)(b) follows directly from the displayed exact sequence in Proposition 2.3.1(iii).

The equivalence of condition (i)(b) and (i)(c) relies on the fact that $\mathbb{Q}_p[G]$ is a semisimple $\mathbb{Q}_p$-algebra. In particular, whilst the exact sequence (3.1) implies that the $\mathbb{Q}_p[G]$-modules $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A_L^\Sigma$ and $(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_L^\Sigma) \oplus \mathbb{Q}_p$ are isomorphic, the results of Proposition 2.3.1(iii) and (iv) combine to imply $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A_L^\Sigma$ is also isomorphic to $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Q}_p(1)) \oplus \mathbb{Q}_p$, and hence that $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_L^\Sigma$ and $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Q}_p(1))$ are isomorphic $\mathbb{Q}_p[G]$-modules.

This makes clear the implication from (i)(b) to (i)(c) and also implies the converse since $\ker(\lambda_{L,p})$ is $\mathbb{Z}_p$-free, and so the exact sequence in Proposition 2.3.1(iii) implies that condition (i)(b) is satisfied if and only if $H^1_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Q}_p(1))$ and $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} W_{L,p}$ are isomorphic $\mathbb{Q}_p[G]$-modules.

To prove claim (ii) we note that if no archimedean place of K ramifies in L, then $W_{L,p}$ is a free $\mathbb{Z}_p[G]$-module of rank equal to $\mathrm{rk}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_{\mathbb{Z}} W'_K) = r_K$, we have $r_L = |G| \cdot r_K$ and Leopoldt's Conjecture for L at p is valid if and only if $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot B_L^\Sigma) = |G| \cdot r_K$.

In particular, since the validity of Leopoldt's Conjecture is inherited by subfields the implication from (ii)(a) to (ii)(b) follows directly from claim (i).

Next we see that, under the conditions of (ii)(b), one has $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_K^\Sigma) = r_K$ and $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_L^\Sigma) = |G| \cdot \dim_{\mathbb{Q}_p}(H_0(G, \mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_L^\Sigma))$. To prove (ii)(c) it is therefore enough to show $\dim_{\mathbb{Q}_p}(H_0(G, \mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_L^\Sigma)) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_K^\Sigma)$ and this follows immediately from Lemma 3.3.2(i) below.

Finally, the condition (ii)(c) implies that $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_L^\Sigma) = |G| \cdot r_K = r_L$ and hence (ii)(a) is true. $\square$

Lemma 3.3.2. Let L/K, Σ and G be as in Proposition 3.3.1.

(i) Then the spaces $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H_0(G, A_L^\Sigma)$ and $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H_0(G, B_L^\Sigma)$ identify with $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A_K^\Sigma$ and $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} B_K^\Sigma$ respectively.

(ii) If G is cyclic of p-power order, then $H_0(G, A_L^\Sigma)$ identifies with $\mathrm{Gal}(M_K^\Sigma/L)$.

(iii) If L is contained in K^{cyc}, then $H_0(G, B_L^\Sigma)$ identifies with B_K^Σ.

Proof. In view of Lemma 2.3.1(iii), claim (i) for the group A_L^Σ asserts that $H^2_{c,\text{ét}}(\mathcal{O}_{K,\Sigma}, \mathbb{Q}_p(1))$ identifies with the G-coinvariants of $H^2_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Q}_p(1))$ and this is a standard consequence of the canonical descent isomorphism $\mathbb{Z}_p \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G]} R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1)) \cong R\Gamma_{c,\text{ét}}(\mathcal{O}_{K,\Sigma}, \mathbb{Z}_p(1))$ in étale cohomology.

To deduce the analogous result for B_L^Σ it suffices to observe that the short exact sequence of $\mathbb{Q}_p[G]$-modules that is induced by (3.1) splits since $\mathbb{Q}_p[G]$ is semisimple.

If G is cyclic, then Galois theory identifies $H_0(G, A_L^\Sigma)$ with $\mathrm{Gal}(E/L)$ where E is the maximal extension of L inside M_L^Σ that is abelian over K. Claim (ii) is therefore true because if G has p-power order, then $E = M_K^\Sigma$.

To prove claim (iii) we assume that $L \subset K^{\mathrm{cyc}}$ and recall that the exact sequence (3.1) splits in this case (by Corollary 3.2.4). Since this sequence splits, the result in claim (ii) identifies $H_0(G, B_L^\Sigma)$ with the kernel $\mathrm{Gal}(M_K^\Sigma/L^{\mathrm{cyc}})$ of the restriction map $\mathrm{Gal}(M_K^\Sigma/L) \to \Gamma_L$ and this is equal to B_K^Σ since $K^{\mathrm{cyc}} = L^{\mathrm{cyc}}$. This completes the proof of claim (iii). $\square$

3.4 The proof of Theorem 3.2.1

The following result provides a key reduction step in the proof of Theorem 3.2.1.

Proposition 3.4.1. It is enough to prove Theorem 3.2.1 after replacing condition (i) by the following condition

(i′) For every Galois extension L/K and set of places Σ as in the statement of Theorem 3.2.1, the $\mathrm{Gal}(L/K)$-module $H^1(R\Gamma_{c,\,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1)))$ is cohomologically trivial.

Proof. Set $G := \mathrm{Gal}(L/K)$. We can see that it is enough to show that Leopoldt's Conjecture is valid at p if and only if (i′) is satisfied.

To do this we consider Galois extensions L/K and sets of places Σ as in (i′) and recall that Proposition 2.3.1(iii) gives a short exact sequence of $\mathbb{Z}_p[G]$-modules

$$0 \to W_{L,p} \to H^1(R\Gamma_{c,\,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))) \to \ker(\lambda_{L,p}) \to 0. \tag{3.4}$$

In addition, since the G-module W'_L is free, p is odd and $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is generated by an element τ of order two, the $\mathbb{Z}_p[G]$-module

$$W_{L,p} = H^0(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), W'_L)_p = (1+\tau)\cdot W'_{L,p}$$

is a direct summand of $W'_{L,p} = (1+\tau)\cdot W'_{L,p} \oplus (1-\tau)\cdot W'_{L,p}$ and so is projective, and hence cohomologically trivial.

From the exact sequence (3.4) it follows that the G-module $H^1(R\Gamma_{c,\,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1)))$ is cohomologically trivial if and only if $\ker(\lambda_{L,p})$ is cohomologically trivial.

Now, if Leopoldt's Conjecture is valid at p, then $\ker(\lambda_{L,p})$ vanishes and so the module $H^1(R\Gamma_{c,\,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1)))$ must be cohomologically trivial.

On the other hand, if each module $\ker(\lambda_{L,p})$ is cohomologically trivial, then the Tate cohomology group $\hat{H}^0(G, \ker(\lambda_{L,p}))$ vanishes and so

$$\left(\sum_{g\in G} g\right)(\ker(\lambda_{L,p})) = H^0(G, \ker(\lambda_{L,p})) = \ker(\lambda_{K,p}), \tag{3.5}$$

where the last equality is valid because we have that both $H^0(G, \mathcal{O}_L^\times) = \mathcal{O}_K^\times$ and $H^0(G, (\mathcal{O}_{L_w}^\times)_p^\times) = (\mathcal{O}_{K_v}^\times)_p^\times$ for each p-adic place w of L lying over a place v of K.

The above equality is equivalent to saying that the homomorphism

$$\pi_{L/K} : \ker(\lambda_{L,p}) \to \ker(\lambda_{K,p})$$

induced by taking field-theoretic norms is surjective for every Galois extension of number fields L/K.

It is therefore now enough to recall that in [12, Lemma 5.3] Burns and Macias Castillo have shown that the validity of Leopoldt's Conjecture at p will follow from the surjectivity of the maps π_{L_{n+1}/L_n} for all number fields L and all sufficiently large integers n, where L_a is the subextension of L^{cyc} of degree p^a over L. $\square$

Now we must show that condition (i$'$) in Proposition 3.4.1 is equivalent to conditions (ii) and (iii) in Theorem 3.2.1. We set $C^\bullet := R\Gamma_{c,\text{ét}}(\mathcal{O}_{L,\Sigma}, \mathbb{Z}_p(1))$.

To show the equivalence of (i$'$) and (ii) we use the fact that, as a special case of (2.1), there is an exact triangle in $D(\mathbb{Z}_p[G])$ of the form

$$\tau^{\leq 1}C^\bullet \to C^\bullet \to \tau^{\geq 2}C^\bullet \to .$$

Since $C^\bullet$ is a perfect complex (by Proposition 2.3.1(i)), this triangle shows that $\tau^{\geq 2}C^\bullet$ is perfect if and only if $\tau^{\leq 1}C^\bullet$ is perfect.

Now the only non-zero cohomology group of $\tau^{\leq 1}C^\bullet$ occurs in degree one (by Proposition 2.3.1(ii)) and this module is finitely generated over $\mathbb{Z}_p$ and so Lemma 2.2.3 implies that $\tau^{\leq 1}C^\bullet$ is perfect over $\mathbb{Z}_p[G]$ if and only if the G-module $H^1(\tau^{\leq 1}C^\bullet) = H^1(C^\bullet)$ is cohomologically trivial. This shows the equivalence of the conditions (i$'$) and (ii).

To show the equivalence of the conditions (ii) and (iii) in Theorem 3.2.1 we note that, by a standard construction of homological algebra, in the exact sequence of $\mathbb{Z}_p[G]$-modules (3.3) we can assume that D^2 is finitely generated and that D^3 is both finitely generated and free. From now on, we write M for D^2 and P for D^3.

Now since P is a free $\mathbb{Z}_p[G]$-module, the argument of Lemma 2.2.3 implies that $\tau^{\geq 2}C$ belongs to $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$ if and only if the G-module M is cohomologically trivial.

By [5, VI, Theorem 8.9], it follows that $\tau^{\geq 2}C$ belongs to $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$ if any only if for all subgroups J of G one has $\hat{H}^i(J, M) = 0$ for both $i = 1$ and $i = 2$.

To understand this condition we use the fact that, in this case, the exact sequence (3.3) gives rise to two short exact sequences of $\mathbb{Z}_p[G]$-modules

$$\begin{cases} 0 \to A_L^\Sigma \to M \to \mathrm{Im}(d) \to 0 \\ \\ 0 \to \mathrm{Im}(d) \to P \to \mathbb{Z}_p \to 0 \end{cases} \tag{3.6}$$

and hence for all subgroups J of G to two long exact sequences of Tate cohomology

$$\begin{aligned} \cdots \to \hat{H}^0(J, \mathrm{Im}(d)) \xrightarrow{\kappa^0_{J,1}} \hat{H}^1(J, A_L^\Sigma) \to \hat{H}^1(J, M) \to \\ \hat{H}^1(J, \mathrm{Im}(d)) \xrightarrow{\kappa^1_{J,1}} \hat{H}^2(J, A_L^\Sigma) \to \hat{H}^2(J, M) \to \hat{H}^2(J, \mathrm{Im}(d)) \xrightarrow{\kappa^2_{J,1}} \dots \end{aligned} \tag{3.7}$$

and

$$\begin{aligned} \cdots \to \hat{H}^0(J, \mathbb{Z}_p) \xrightarrow{\kappa^0_{J,2}} \hat{H}^1(J, \mathrm{Im}(d)) \to \hat{H}^1(J, P) \to \\ \hat{H}^1(J, \mathbb{Z}_p) \xrightarrow{\kappa^1_{J,2}} \hat{H}^2(J, \mathrm{Im}(d)) \to \hat{H}^2(J, P) \to \hat{H}^2(J, \mathbb{Z}_p) \xrightarrow{\kappa^2_{J,2}} \dots \end{aligned} \tag{3.8}$$

These exact sequences show that the required vanishing of $\hat{H}^i(J, M)$ for all subgroups J and for $i = 1$ and $i = 2$ is equivalent to requiring that

$$\kappa^0_{J,1} \text{ is surjective, } \kappa^1_{J,1} \text{ is bijective and } \kappa^2_{J,1} \text{ is injective.} \tag{3.9}$$

We have:

$$\hat{H}^i(J, \mathbb{Z}_p) \cong \begin{cases} 0 & \text{if } i = -1, i = 1 \\ \\ \mathbb{Z}_p/|J| & \text{if } i = 0. \end{cases}$$

Since each homomorphism $\kappa^i_{J,2}$ in (3.8) is bijective (since the module P that occurs in (3.6) is a free $\mathbb{Z}_p[G]$-module, and hence cohomologically trivial), these facts mean that the exact sequence (3.7) can be written as follows:

$$\cdots \to 0 \xrightarrow{\kappa^0_{J,1}} \hat{H}^1(J, A^\Sigma_L) \to \hat{H}^1(J, M) \to$$
$$\mathbb{Z}_p/|J| \xrightarrow{\kappa^1_{J,1}} \hat{H}^2(J, A^\Sigma_L) \to \hat{H}^2(J, M) \to 0 \xrightarrow{\kappa^2_{J,1}} \cdots.$$

From this, we can see that $\kappa^2_{J,1}$ is injective, that $\kappa^0_{J,1}$ is surjective if and only if $\hat{H}^1(J, A^\Sigma_L)$ vanishes and that $\kappa^1_{J,1}$ is bijective if and only if $(\kappa^1_{J,1} \circ \kappa^0_{J,2})(1_{|J|})$ both has order $|J|$ and generates $\hat{H}^2(J, A^\Sigma_L)$ (where $1_{|J|}$ denotes the image of 1 in $\mathbb{Z}_p/|J|$).

In addition, the composite $\kappa^1_{J,1} \circ \kappa^0_{J,2}$ coincides, up to a sign, with the map given by taking cup product with the element $c^{\Sigma,\text{ét}}_{L/L^J}$ of

$$\hat{H}^2(J, A^\Sigma_L) = H^2(J, A^\Sigma_L) \cong \mathrm{YExt}^2_J(\mathbb{Z}_p, A^\Sigma_L)$$

that corresponds to $\tau^{\geq 2}C^\bullet$, considered (by restriction) as a complex of $\mathbb{Z}_p[J]$-modules, and so we have $(\kappa^1_{J,1} \circ \kappa^0_{J,2})(1_{|J|}) = \pm c^{\Sigma,\text{ét}}_{L/L^J}$. The required bijectivity of the map $\kappa^1_{J,1}$ is therefore equivalent to Theorem 3.2.1(iii)(b).

To complete the proof of Theorem 3.2.1(iii) it remains to show that the group $\hat{H}^1(J, A^\Sigma_L)$ vanishes if and only if the cyclotomic extension class $c^{\Sigma,\gamma_L}_{L/L^J}$ generates $H^1(J, B^\Sigma_L)$.

This time, the equivalence is a consequence of the fact that $H^1(J, \mathbb{Z}_p)$ vanishes and the long exact sequence of Tate cohomology of (3.1) gives an exact sequence of abelian groups

$$\hat{H}^0(J, \mathbb{Z}_p) \xrightarrow{\alpha} H^1(J, B^\Sigma_L) \to H^1(J, A^\Sigma_L) \to H^1(J, \mathbb{Z}_p)$$

in which α sends the element $1_{|J|}$ of $\hat{H}^0(J, \mathbb{Z}_p) = \mathbb{Z}_p/|J|$ to $c^{\Sigma,\gamma_L}_{L/L^J}$.

This completes the proof of Theorem 3.2.1.

3.5 The proof of Corollary 3.2.3

We fix L/K and Σ as in the statement of Corollary 3.2.3, set $G := \mathrm{Gal}(L/K)$ and assume that L validates Leopoldt's Conjecture at p.

The implication from (ii) to (i) is clear since if B_L^Σ is a cohomologically trivial G-module, then $H^1(G, B_L^\Sigma)$ vanishes and so the sequence (3.1) splits.

Next note that if (3.1) splits, then in each degree i and for each p-subgroup J of G there are isomorphisms of Tate cohomology groups

$$\hat{H}^{i-2}(J, \mathbb{Z}_p) \cong \hat{H}^i(J, A_L^\Sigma) \cong \hat{H}^i(J, B_L^\Sigma) \oplus \hat{H}^i(J, \mathbb{Z}_p). \tag{3.10}$$

Here, the first map is the composite $\kappa_{J,1}^{i-1} \circ \kappa_{J,2}^{i-2}$ of the connecting homomorphisms that occur in (3.7) and (3.8) and is an isomorphism since the assumed validity of Leopoldt's Conjecture for L at p implies that both of the modules M and P that occur in the proof of Theorem 3.2.1 are cohomologically trivial and hence that the maps $\kappa_{J,1}^{i-1}$ and $\kappa_{J,2}^{i-2}$ are both bijective.

Now if $i = 0$, then the map (3.10) is an isomorphism between the abelianization $J^{\mathrm{ab}} \cong \hat{H}^{-2}(J, \mathbb{Z}_p)$ of J and the group $\hat{H}^0(J, B_L^\Sigma) \oplus \mathbb{Z}_p/|J|$ and so induces a surjective homomorphism from J^{ab} to $\mathbb{Z}_p/|J|$.

The existence of such a surjective homomorphism implies both that J is cyclic and that $\hat{H}^0(J, B_L^\Sigma)$, and hence (since the Tate cohomology of cyclic groups is periodic of order two) also $\hat{H}^a(J, B_L^\Sigma)$ in every even degree a, vanishes.

In a similar way, the vanishing of $\hat{H}^{-1}(J, \mathbb{Z}_p)$ combines with (3.10) to imply the vanishing of $\hat{H}^a(J, B_L^\Sigma)$ in every odd degree a.

This shows that B_L^Σ is a cohomologically trivial J-module for any p-subgroup J of G and hence also a cohomologically trivial G-module (by [5, Chapter VI, Proposition (8.8)]), which shows the implication from (i) to (ii).

It now remains to prove the equivalence of the conditions (ii) and (iii) and to do this we fix a Sylow p-subgroup J of G and set $F := L^J$.

Noting that condition (ii) implies that J is cyclic (by the above argument) and that the same is clearly true under condition (iii)(a) and by assumption under condition (iii)(b), we will assume in the rest of the proof that J is cyclic.

In particular, since B_L^Σ spans a free $\mathbb{Q}_p[J]$-module (by Proposition 3.3.1(ii)), in this case a Herbrand quotient argument combines with [5, Chapter VI, Proposition (8.8)] to imply that B_L^Σ is a cohomologically trivial G-module if and only if for each non-trivial subgroup C of J the Tate cohomology group $\hat{H}^{-1}(C, B_L^\Sigma) \cong H^1(C, B_L^\Sigma)$ vanishes.

In addition, if $L \subseteq F^{\mathrm{cyc}}$, then Corollary 3.2.4 implies that (3.1) splits as a sequence of $\mathbb{Z}_p[J]$-modules and hence, by Theorem 3.2.1 and the assumed validity of Leopoldt's Conjecture for L at p, that each group $H^1(C, B_L^\Sigma)$ vanishes.

In the following we will hence assume both that J is cyclic and that $L \not\subset F^{\mathrm{cyc}}$ and we need to show, under these hypotheses, that the conditions in (iii)(b) are satisfied if and only if the J-module B_L^Σ is cohomologically trivial, or equivalently that $\hat{H}^{-1}(C, B_L^\Sigma)$ vanishes for each non-trivial subgroup C of J.

We can also assume both $L \cap K^{\mathrm{cyc}} = K$ and that for each subgroup C as above, with $E := L^C$, the maximal abelian extension of E^{cyc} in M_L^Σ is equal to M_E^Σ since these conditions are explicitly assumed in (iii)(b) and also follow from the cohomological triviality of B_L^Σ by Lemma 3.5.1 below (with L/K replaced by L/F).

Now, since C is cyclic, the last assumption implies that the restriction map $B_L^\Sigma = \mathrm{Gal}(M_L^\Sigma/L^{\mathrm{cyc}}) \to \mathrm{Gal}(M_E^\Sigma/L^{\mathrm{cyc}})$ induces an identification of $H_0(C, B_L^\Sigma)$ with $\mathrm{Gal}(M_E^\Sigma/L^{\mathrm{cyc}})$.

In addition, the finite group $\hat{H}^{-1}(C, B_L^\Sigma)$ is equal (by definition) to the kernel of the map

$$T_C : \mathrm{Gal}(M_E^\Sigma/L^{\mathrm{cyc}}) = H_0(C, B_L^\Sigma) \to B_L^\Sigma$$

that is induced by the action of $\sum_{c\in C} c$ on B_L^Σ and so vanishes if and only if T_C is injective on the torsion subgroup of $\mathrm{Gal}(M_E^\Sigma/L^{\mathrm{cyc}})$.

Under our hypotheses, the equivalence of the conditions (ii) and (iii)(b) is therefore a consequence of the fact that the explicit definition of transfer maps implies that T_C is equal to the restriction to $\mathrm{Gal}(M_E^\Sigma/L^{\mathrm{cyc}})$ of the transfer map from $A_E^\Sigma = \mathrm{Gal}(M_E^\Sigma/E) = \mathrm{Gal}(M_L^\Sigma/E)^{\mathrm{ab}}$ to $\mathrm{Gal}(M_L^\Sigma/L)^{\mathrm{ab}} = \mathrm{Gal}(M_L^\Sigma/L) = A_L^\Sigma$.

This completes the proof of Corollary 3.2.3.

Lemma 3.5.1. Let L/K be a cyclic extension of number fields of p-power degree with Galois group G that is unramified outside a finite set of places Σ of K that contains all archimedean and p-adic places. Moreover, we also assume that B_L^Σ is a cohomologically trivial G-module.

Then the following claims are valid.

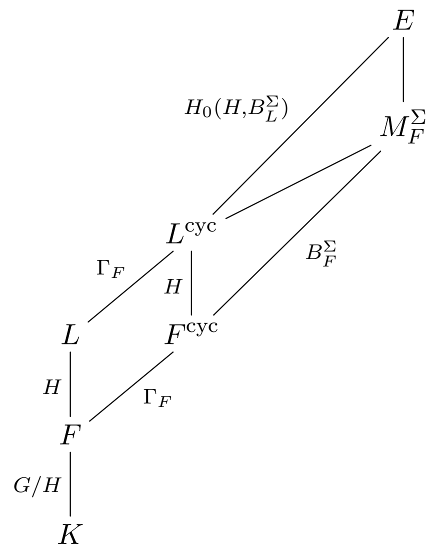
(i) For any subgroup H of $\mathrm{Gal}(L/L\cap K^{\mathrm{cyc}})$, with $F := L^H$, the maximal abelian extension of F^{cyc} in M_L^Σ is equal to M_F^Σ and hence $H_0(H, B_L^\Sigma)$ identifies with $\mathrm{Gal}(M_F^\Sigma/L^{\mathrm{cyc}})$.

(ii) If $L\cap K^{\mathrm{cyc}}$ validates Leopoldt's Conjecture at p, then either $L \subseteq K^{\mathrm{cyc}}$ or $L\cap K^{\mathrm{cyc}} = K$.

Proof. With H and F as in claim (i) we write E for the maximal abelian extension of F^{cyc} in M_L^Σ.

One has $L\cap F^{\mathrm{cyc}} = F$ so the natural restriction maps give identifications $\Gamma_L = \Gamma_F$ and $\mathrm{Gal}(L^{\mathrm{cyc}}/F^{\mathrm{cyc}}) = H$.

Then, since H is cyclic, the conjugation action of H on B_L^Σ identifies $\mathrm{Gal}(E/L^{\mathrm{cyc}})$ with $H_0(H, B_L^\Sigma)$ and so gives a field diagram:



Now, since B_L^Σ is assumed to be cohomologically trivial, the exact sequence (3.1) splits and hence induces an identification of $\mathrm{Gal}(E/L^{\mathrm{cyc}}) = H_0(H, B_L^\Sigma)$ with the kernel of the restriction map $H_0(H, A_L^\Sigma) \to H_0(H, \Gamma_L) = \Gamma_L$. Since the restriction map $A_L^\Sigma \to A_F^\Sigma$ induces an identification of $H_0(H, A_L^\Sigma)$ with $\mathrm{Gal}(M_F^\Sigma/L)$ (by Lemma 3.3.2(ii)) this implies that $E = M_F^\Sigma$, and hence that $H_0(H, B_L^\Sigma) = \mathrm{Gal}(M_F^\Sigma/L^{\mathrm{cyc}})$, as required to prove claim (i).

To prove claim (ii) we assume that $L \not\subseteq K^{\mathrm{cyc}}$ and set $F := L \cap K^{\mathrm{cyc}}$ so that the subgroup $H := \mathrm{Gal}(L/F)$ is both non-trivial and naturally isomorphic to $\mathrm{Gal}(L^{\mathrm{cyc}}/F^{\mathrm{cyc}})$. Then the above argument gives a short exact sequence of $\mathbb{Z}_p[G/H]$-modules

$$0 \to H_0(H, B_L^\Sigma) \to B_F^\Sigma \to \mathrm{Gal}(L^{\mathrm{cyc}}/F^{\mathrm{cyc}}) \to 0 \tag{3.11}$$

where G/H acts trivially on $\mathrm{Gal}(L^{\mathrm{cyc}}/F^{\mathrm{cyc}})$.

Now the cohomological triviality of B_L^Σ as a G-module implies that $H_0(H, B_L^\Sigma) \cong H^0(H, B_L^\Sigma)$ is a cohomologically trivial G/H-module. In addition, if F validates Leopoldt's Conjecture at p, then (since $F \subseteq K^{\mathrm{cyc}}$) the implication from Corollary 3.2.3(iii)(a) to Corollary 3.2.3(ii) (with L/K replaced by F/K) above implies that B_F^{Σ} is a cohomologically trivial G/H-module.

From the exact sequence (3.11) it therefore follows that the G/H-module $\mathrm{Gal}(L^{\mathrm{cyc}}/F^{\mathrm{cyc}}) \cong H \cong \mathbb{Z}_p/|H|$ is cohomologically trivial and, as p divides $|H|$, this is only possible if G/H is the trivial group and hence $F = K$. This proves claim (ii). $\square$

Chapter 4

Ray class groups over cyclic p-extensions

To discuss the Galois structures of ray class groups in greater detail, in this chapter we restrict our attention to cyclic Galois extensions of number fields of p-power degree.

In this special case we explain how to use an important representation-theoretic result of Yakovlev to establish new results concerning the explicit Galois structure of the groups A_L^{Σ}.

Throughout this chapter we fix a cyclic extension of number fields L/K of degree p^n for some natural number n and a finite set of places Σ of K that contains all archimedean and p-adic places and all places that ramify in L/K.

For each integer i with $0 \leq i \leq n$ we write L_i for the unique extension of K in L for which $[L : L_i] = p^i$. For each such intermediate field F of L/K we define

$$T_{L/F}^{\Sigma} := \mathrm{cok}(\mathrm{Gal}(M_L^{\Sigma}/L)_{\mathrm{tor}} \xrightarrow{\pi_{L/F}} \mathrm{Gal}(M_F^{\Sigma}/L)_{\mathrm{tor}})$$

where $\pi_{L/F}$ is induced by the natural restriction map.

This is a finite group which is isomorphic to the torsion subgroup of $\mathrm{Gal}((L^{\max} \cap M_F^{\Sigma})/L)$ where $L^{\max}$ is the maximal $\mathbb{Z}_p$-power extension of L (see Lemma 4.5.4 below).

4.1 Statement of the main results

We recall that for any number field E we write r_E for the number of its complex places and δ_E for its p-adic 'Leopoldt defect'.

We recall also that δ_E is a non-negative integer which vanishes if and only if Leopoldt's Conjecture is valid for E at p and that there are equalities

$$\mathrm{rk}_{\mathbb{Z}_p}(B_E^{\Sigma}) = \mathrm{rk}_{\mathbb{Z}_p}(A_E^{\Sigma}) - 1 = r_E + \delta_E \tag{4.1}$$

(cf. [33, (10.3.7) Corollary]).

We now state the main result that will be proved in this chapter.

Theorem 4.1.1. Let L/K and Σ be as above and set $G := \mathrm{Gal}(L/K)$.

Then the isomorphism class of the $\mathbb{Z}_p[G]$-module $\overline{A_L^{\Sigma}}$ is determined (in a sense to be made precise in Theorem 4.2.1 below) by r_K, the Leopoldt defects δ_{L_i} for each i with $0 \le i \le n$ and the diagrams of finite groups

$$\begin{cases} T^{\Sigma}_{L/L_1} \xrightarrow{f_{L_1,L_2}} T^{\Sigma}_{L/L_2} \xrightarrow{f_{L_2,L_3}} \dots \xrightarrow{f_{L_{n-1},L_n}} T^{\Sigma}_{L/L_n} \\ T^{\Sigma}_{L/L_1} \xleftarrow{g_{L_2,L_1}} T^{\Sigma}_{L/L_2} \xleftarrow{g_{L_3,L_2}} \dots \xleftarrow{g_{L_n,L_{n-1}}} T^{\Sigma}_{L/L_n}. \end{cases} \tag{4.2}$$

Here, each homomorphism $f_{L_i,L_{i+1}}$ is induced by the natural restriction map

$$\mathrm{Gal}(M^{\Sigma}_{L_i}/L) \to \mathrm{Gal}(M^{\Sigma}_{L_{i+1}}/L)$$

and each homomorphism g_{L_{i+1},L_i} by the map

$$\mathrm{Gal}(M^{\Sigma}_{L_{i+1}}/L) \to \mathrm{Gal}(M^{\Sigma}_{L_i}/L),$$

which sends x to $\sum_{c \in \mathrm{Gal}(L_i/L_{i+1})} c(\tilde{x})c^{-1}$ where $\tilde{x}$ is any lift of x to $\mathrm{Gal}(M^{\Sigma}_{L_i}/L)$.

Remark 4.1.2. The groups $A^{\Sigma}_{L,\mathrm{tor}}$ have already been extensively studied in the literature (see, in particular, the computations of Hemard in [22]) and using these results one can often explicitly compute the groups $T^{\Sigma}_{L/F}$ that occur in Theorem 4.1.1. For an example of such a computation see the proof of Lemma 7.2.3 below.

In the first of these results we characterise the vanishing of the groups T^{Σ}_{L/L_i} in terms of the explicit structure of A^{Σ}_{L}.

Corollary 4.1.3. Let L/K and Σ be as above. We write ε for the identity element of G.

(i) The groups T^{Σ}_{L/L_i} vanish for all intermediate fields L_i if and only if there exists, for each subgroup H of G, a non-negative integer n_H for which there is an isomorphism of $\mathbb{Z}_p[G]$-modules of the form
$$\overline{A^{\Sigma}_{L}} \cong \bigoplus_{H \leq G} \mathbb{Z}_p[G/H]^{n_H}.$$

(ii) If the conditions in claim (i) are satisfied and, in addition, Leopoldt's Conjecture is valid for K at p, then $n_{\{\varepsilon\}} \geq r_K$ and if $n_{\{\varepsilon\}} = r_K$ then there exists a unique subgroup H' of G such that $n_{H'} = 1$ and $n_H = 0$ for all $H \neq H'$.

(iii) If the conditions in claim (ii) are satisfied and, in addition, Leopoldt's Conjecture is valid for L at p, then one has $n_{\{\varepsilon\}} = r_K$ and $H' = G$ and so $\overline{A^{\Sigma}_{L}}$ is isomorphic to $\mathbb{Z}_p[G]^{r_K} \oplus \mathbb{Z}_p$.

Remark 4.1.4. For any intermediate field E of L/K it is clear that the group $T^{\Sigma}_{L/E}$ vanishes whenever the ray class group A^{Σ}_{E} is torsion-free. In addition, in the case that Σ contains just archimedean and p-adic places Gras has characterised, assuming the validity of Leopoldt's Conjecture at p, those fields E for which A^{Σ}_{E} is torsion-free (see [19, Theorem I 2, Corollary 1]). One can also characterise the vanishing of $T^{\Sigma}_{L/E}$ in terms of so-called '$\mathbb{Z}_p$-extendable' extensions (see the discussion in §4.5 below).

Remark 4.1.5. If L/K is a cyclic extension of degree either p or p^2, then the indecomposable $\mathbb{Z}_p[G]$-lattices have been classified explicitly by Diederichsen [15] and by Heller and Reiner [20] respectively and these classifications can be used to give a much more explicit version of Theorem 4.1.1. If L/K has degree p such an analysis has already been made by Miki and Sato in [31] (see the proof of Proposition 6.2.1 below for more details). However, if L/K has degree p^2 the analysis is much more involved and will be discussed in greater detail, but with only partial success, in Chapter 5.

In the next result, we discuss a case where we can use Theorem 4.1.1 to establish an upper bound on the number of isomorphism classes of indecomposable $\mathbb{Z}_p[G]$-modules that can occur in the Krull-Schmidt decomposition of modules of the form $\overline{A^{\Sigma}_{L}}$.

To state this result we write C_n for each non-negative integer n for the cyclic group of order p^n. For each non-negative integer m with $m \leq n$ we regard C_m as a quotient of C_n in the obvious way, and fix a set $\mathrm{IM}_{p,n}$ of representatives of the isomorphism classes of all indecomposable $\mathbb{Z}_p[C_n]$-lattices that are not isomorphic to $\mathbb{Z}_p[C_m]$ for any m with $0 \leq m \leq n$.

Let F/E a profinite extension of number fields that is unramified outside p. For each natural number n and each lattice I in $\mathrm{IM}_{p,n}$, define $m_I(\overline{A^{p}_{L}})$ to be the multiplicity with which the isomorphism class of I occurs as a direct summand of $\overline{A^{p}_{L}}$ when A^{p}_{L} is regarded as a $\mathbb{Z}_p[C_n]$-module via some choice of isomorphism of $\mathrm{Gal}(L/K)$ with C_n. We then set

$$m_I(F/E) := \max\{m_I(\overline{A_L^p})\}_{L/K}$$

where L/K ranges over cyclic extensions of degree p^n with $E \subseteq K \subset L \subset F$ and K/E finite.

Remark 4.1.6. Whilst there is no reason for $m_I(F/E)$ to always be well-defined (since the terms $m_I(\overline{A_L^p})$ can be unbounded as the extensions L/K vary), we study a natural class of profinite extensions F/E for which $m_I(F/E)$ is well defined.

For each natural number b we also set

$$\kappa_n^b := \sum_{J_1\times\cdots\times J_n} \prod_{i=1}^{i=n-1} c_{J_i} c_{J_{i+1}},$$

where in the sum each J_i runs over a set of representatives of the isomorphism classes of finite abelian p-groups of exponent dividing p^i and p-rank at most b and c_{J_i} denotes the number of conjugacy classes in $\mathrm{Aut}(J_i)$ comprising elements of order dividing p^n.

Corollary 4.1.7. Let E_∞ be a $\mathbb{Z}_p$-extension of a number field E for which all p-adic places of E have open decomposition groups in $\mathrm{Gal}(E_\infty/E)$ and the Iwasawa μ-invariant of the extension $E_\infty(\zeta_p)/E(\zeta_p)$ vanishes, where ζ_p is a choice of primitive p-th root of unity in $\mathbb{Q}^c$. Let F be a finite p-extension of E_∞ that is both unramified outside p and Galois over E.

Then each integer $m_I(F/E)$ is well-defined and there exists an integer d which depends only on F/E and is such that

$$\sum_{I\in \mathrm{IM}_{p,n}} m_I(F/E) \leq p^{n(n-1)d^2} \cdot \kappa_n^d. \tag{4.3}$$

In particular, only finitely many isomorphism classes of indecomposable $\mathbb{Z}_p[C_n]$-lattices can occur as direct summands of $\overline{A_L^p}$ as L/K runs over the infinitely many cyclic degree p^n

extensions for which $E \subseteq K \subset L \subset F$ and K/E finite and, in each case, $\overline{A_L^p}$ is regarded as a C_n-module via some choice of isomorphism of $\mathrm{Gal}(L/K)$ with C_n.

Remark 4.1.8. Corollary 4.1.7 is of interest for the following reason. By definition, the set $\mathrm{IM}_{p,n}$ does not include modules of the form $\mathbb{Z}_p[C_m]$ for any integer m with $0 \le m \le n$. Since these finitely many indecomposable modules may also occur as direct summands of $\overline{A_L^p}$, the bound given in (4.3) does not prevent the $\mathbb{Z}_p$-rank of $\overline{A_L^p}$ being unbounded as L/K ranges over the given set of fields. In addition, if $n > 2$, then Heller and Reiner [21] have shown that $\mathrm{IM}_{p,n}$ is infinite (and there is still no explicit description of these sets!) and so, in principle, infinitely many non-isomorphic indecomposable modules could occur as direct summands of $\overline{A_L^p}$ as L/K ranges over the given set of fields.

4.2 The proof of Theorem 4.1.1

We start by recalling the result of Yakovlev that will be key to our argument.

Theorem 4.2.1 (Yakovlev [39])**.** Let Γ be a cyclic group of order p^n and for each integer i with $0 \le i \le n$ write Γ_i for its subgroup of order p^i.

If M and M' are finitely generated $\mathbb{Z}_p[\Gamma]$-lattices for which, for each integer i with $1 \le i \le n$, there are isomorphisms of $\mathbb{Z}_p[\Gamma/\Gamma_i]$-modules $\theta_i : \hat{H}^{-1}(\Gamma_i, M) \to \hat{H}^{-1}(\Gamma_i, M')$ that lie in commutative diagrams

$$\begin{tikzcd} \hat{H}^{-1}(\Gamma_i, M) \arrow[r, "\mathrm{cor}"] \arrow[d, "\theta_i"'] & \hat{H}^{-1}(\Gamma_{i+1}, M) \arrow[d, "\theta_{i+1}"] \\ \hat{H}^{-1}(\Gamma_i, M') \arrow[r, "\mathrm{cor}"] & \hat{H}^{-1}(\Gamma_{i+1}, M') \end{tikzcd}$$

$$\begin{tikzcd} \hat{H}^{-1}(\Gamma_i, M) \arrow[d, "\theta_i"'] & \hat{H}^{-1}(\Gamma_{i+1}, M) \arrow[l, "\mathrm{res}"'] \arrow[d, "\theta_{i+1}"] \\ \hat{H}^{-1}(\Gamma_i, M') & \hat{H}^{-1}(\Gamma_{i+1}, M'), \arrow[l, "\mathrm{res}"'] \end{tikzcd} \tag{4.4}$$

where 'res' and 'cor' denote the natural restriction and corestriction maps, then there are isomorphisms of $\mathbb{Z}_p[\Gamma]$-modules of the form

$$M \cong M_1 \oplus M_2 \text{ and } M' \cong M_1' \oplus M_2' \tag{4.5}$$

where the modules M_1 and M_1' are isomorphic and the modules M_2 and M_2' are both direct sums of modules of the form $\mathbb{Z}_p[\Gamma/\Delta]$ for suitable subgroups Δ of Γ.

Remark 4.2.2. An important special case of Theorem 4.2.1 arises when the group $\hat{H}^{-1}(\Gamma_i, M)$ vanishes for all i. In this case the conditions of Theorem 4.2.1 are satisfied by taking $M' = 0$ and so the isomorphisms (4.5) imply that M_1', and hence M_1, vanishes and so $M = M_2$ is a direct sum of modules of the form $\mathbb{Z}_p[G/H]$ for suitable subgroups H of G. Such modules M are known as 'permutation modules'.

Remark 4.2.3. Theorem 4.2.1 says that a finitely generated $\mathbb{Z}_p[\Gamma]$-lattice M is determined, up to isomorphism and the addition of permutation modules, by the collection of diagrams (4.4). Given the well-known difficulty of classifying indecomposable $\mathbb{Z}_p[\Gamma]$-modules, this is a very strong result. To prove it Yakovlev uses the given maps θ_i to construct homomorphisms of $\mathbb{Z}_p[\Gamma]$-modules $\zeta : M \to M'$ and $\kappa : M' \to M$ (for details see [40, Lemma 5.2]), sets $M_1 := \mathrm{Im}(\kappa)$, $M_2 := \ker(\zeta)$, $M_1' := \mathrm{Im}(\zeta)$ and $M_2' := \ker(\kappa)$ and then shows that M_1 and M_1' are isomorphic and that M_2 and M_2' decompose as the direct sums of modules of the form $\mathbb{Z}_p[\Gamma/\Delta]$. A slightly more general version of Theorem 4.2.1 is proved by Yakovlev in [40].

In the rest of this section we fix the same notation and hypotheses of Theorem 4.1.1. We also set $A := A_L^{\Sigma}$ and $G := \mathrm{Gal}(L/K)$ and for each integer i with $0 \leq i \leq n$ also $G_i := \mathrm{Gal}(L/L_i)$ and $T_i := T_{L/L_i}^{\Sigma}$.

We first clarify the meaning of Theorem 4.2.1 in this setting.

Lemma 4.2.4. Fix an integer i with $0 \leq i \leq n$.

(i) The group T_i is naturally isomorphic as a $\mathbb{Z}_p\big[G/G_i\big]$-module to $\hat{H}^{-1}\big(G_i, \overline{A}\big)$.

(ii) If $i < n$, then the corestriction map $\hat{H}^{-1}\big(G_i, \overline{A}\big) \to \hat{H}^{-1}\big(G_{i+1}, \overline{A}\big)$ corresponds, under the isomorphisms in claim (i), to the homomorphism $T_i \to T_{i+1}$ that is induced by the natural restriction map $A^{\Sigma}_{L_i} \to A^{\Sigma}_{L_{i+1}}$.

(iii) If $i > 0$, then the restriction map $\hat{H}^{-1}\big(G_i, \overline{A}\big) \to \hat{H}^{-1}\big(G_{i-1}, \overline{A}\big)$ corresponds, under the isomorphisms in claim (i), to the homomorphism $T_i \to T_{i-1}$ that is induced by the map $\mathrm{Gal}(M^{\Sigma}_{L_i}/L) \to \mathrm{Gal}(M^{\Sigma}_{L_{i-1}}/L)$ which sends x to $\sum_{c\in \mathrm{Gal}(L_{i-1}/L_i)} c(\tilde{x})$ where $\tilde{x}$ is any lift of x to $\mathrm{Gal}(M^{\Sigma}_{L_{i-1}}/L)$.

Proof. Upon taking G_i-coinvariants of the tautological exact sequence

$$0 \to A_{\mathrm{tor}} \to A \to \overline{A} \to 0,$$

recalling that $H_0(G_i, A)$ identifies with $\mathrm{Gal}(M^{\Sigma}_{L_i}/L)$ (by Lemma 3.3.2(ii)) and then passing to torsion subgroups in the resulting exact sequence one obtains an exact sequence of $\mathbb{Z}_p[G/G_i]$-modules

$$A_{\mathrm{tor}} \xrightarrow{\pi^L_{L_i}} \mathrm{Gal}(M^{\Sigma}_{L_i}/L)_{\mathrm{tor}} \to H_0(G_i, \overline{A})_{\mathrm{tor}} \to 0.$$

Given this exact sequence and the definition of T_i as the cokernel of $\pi^L_{L_i}$, the isomorphism in claim (i) is true if we can show that $H_0(G_i, \overline{A})_{\mathrm{tor}}$ is equal to $\hat{H}^{-1}(G_i, \overline{A})$.

The definition of Tate cohomology gives a natural exact sequence

$$0 \to \hat{H}^{-1}(G_i, \overline{A}) \xrightarrow{\subseteq} H_0(G_i, \overline{A}) \to H^0(G_i, \overline{A}) \to \hat{H}^0(G_i, \overline{A}) \to 0$$

where the third arrow is induced by the action of the element $\sum_{g\in G_i} g$ of $\mathbb{Z}_p[G]$. This implies the equality $H_0(G_i, \overline{A})_{\mathrm{tor}} = \hat{H}^{-1}(G_i, \overline{A})$ since $\hat{H}^{-1}(G_i, \overline{A})$ is finite and $\overline{A}$ is $\mathbb{Z}_p$-free.

This proves claim (i) and, given these isomorphisms, the assertions of claims (ii) and (iii) can be checked by straightforward explicit computation. $\square$

To prove Theorem 4.1.1, we now apply Theorem 4.2.1 with $\Gamma = G$ and $M = \overline{A}$. By Lemma 4.2.4, we see that the top rows of diagrams (4.4) for each integer i correspond to the diagrams that are described in (4.2).

Using Theorem 4.2.1 we can therefore assume that there is a decomposition of $\mathbb{Z}_p[G]$-modules $\overline{A} = R \oplus R'$, where R is uniquely determined up to isomorphism and R' is of the form $\bigoplus_{i=0}^{n} \mathbb{Z}_p[G/G_i]^{a_i}$ for some non-negative integers a_i.

To complete the proof of Theorem 4.1.1, it therefore suffices to show that the isomorphism class of R' is uniquely determined by r_K and the integers δ_{L_i} for each i with $0 \leq i \leq n$.

By Lemma 4.2.5 below, it therefore suffices to show that this data determines the dimension $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, R'))$ for each integer i.

This is true because for each i one has

$$\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, R')) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, A)) - \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, R))$$

and also

$$\begin{aligned} \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, A)) &= \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot A^{\Sigma}_{L_i}) \\ &= r_{L_i} + \delta_{L_i} + 1 \\ &= p^{n-i} \cdot r_K + \delta_{L_i} + 1, \end{aligned}$$

where the first equality is true by Lemma 3.3.2(i) and the second is a consequence of (4.1) with L replaced by L_i.

This completes the proof of Theorem 4.1.1.

Lemma 4.2.5. Any $\mathbb{Z}_p[G]$-module W of the form $\bigoplus_{i=0}^{n} \mathbb{Z}_p[G/G_i]^{a_i}$, where a_i are non-negative integers, is determined up to isomorphism by the integers $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, W))$ for each i with $0 \leq i \leq n$.

Proof. Given the explicit structure of W, the Krull-Schmidt theorem implies that it suffices to show the given dimensions uniquely determine each of the integers a_i for $0 \leq i \leq n$.

But for each such i we can compute that

$$\begin{aligned}
\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, W)) &= \sum_{j=0}^{n} \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, \mathbb{Z}_p[G/G_j]^{a_j}) \\
&= \sum_{j=0}^{n} a_j \cdot \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, \mathbb{Z}_p[G/G_j])) \\
&= \sum_{j=n-i}^{n} a_{n-j} p^{n-i} + \sum_{j=0}^{n-i-1} a_{n-j} p^j,
\end{aligned}$$

where the last equality is true because $H^0(G_i, \mathbb{Z}_p[G/G_j])$ is equal to $\mathbb{Z}_p[G/G_j]$ if $i \leq j$ (and so has $\mathbb{Z}_p$-rank $|G/G_j| = p^{n-j}$) and is isomorphic to $\mathbb{Z}_p[G/G_i]$ if $i > j$ (and so has $\mathbb{Z}_p$-rank $|G/G_i| = p^{n-i}$).

By successively subtracting the above expression from the same expression with i replaced by $i+1$ we find that the dimensions $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H^0(G_i, W))$ do determine all of the integers a_i, as claimed. $\square$

4.3 The proof of Corollary 4.1.3

If the group $T^{\Sigma}_{L/E}$ vanishes for every intermediate field E of L/K, then Lemma 4.2.4(i) implies that the group $\hat{H}^{-1}(H, \overline{A^{\Sigma}_L})$ vanishes for every subgroup H of G.

In this case, therefore, Remark 4.2.2 implies that $\overline{A^{\Sigma}_L}$ is a direct sum of modules of the form $\mathbb{Z}_p[G/H]$ for suitable subgroups H of G. This proves claim (i).

To prove claim (ii) we may assume that $\overline{A_L^\Sigma}$ is isomorphic to a direct sum of the form $\bigoplus_{i=1}^d \mathbb{Z}_p[Q_i]$, where Q_i are certain (not necessarily distinct) quotients of G.

Using this isomorphism we compute that

$$
\begin{aligned}
d &= \sum_{i=1}^{d} \dim_{\mathbb{Q}_p}(\mathbb{Q}_p) \\
&= \sum_{i=1}^{d} \dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p \cdot H^0(G, \mathbb{Z}_p[Q_i])\big) \\
&= \dim_{\mathbb{Q}_p}\left(\mathbb{Q}_p \cdot \bigoplus_{i=1}^{d} H^0(G, \mathbb{Z}_p[Q_i])\right) \\
&= \dim_{\mathbb{Q}_p}(H^0(G, \mathbb{Q}_p \cdot A_L^\Sigma)) \\
&= \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot A_K^\Sigma) \\
&= 1 + r_K,
\end{aligned}
$$

where the fifth equality is a consequence of Lemma 3.3.2(i) and the last follows from (4.1) and our assumption that Leopoldt's Conjecture is valid for K at p (and so $\delta_K = 0$).

Now $r_L = |G| \cdot r_K$ (since no archimedean place ramifies in the odd degree extension L/K) and so the equality $d = 1 + r_K$ combines with (4.1) to imply that

$$
\begin{aligned}
\sum_{i=1}^{1+r_K} |Q_i| &= \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot \overline{A_L^\Sigma}) \\
&= 1 + r_L + \delta_L \\
&= 1 + |G| \cdot r_K + \delta_L \\
&\geq 1 + |G| \cdot r_K.
\end{aligned}
$$

Write d_1 for the number of quotients Q_i equal to G. Then, since $|Q_i| \leq |G|/p$ whenever

$Q_i \neq G$, the above inequality implies

$$1 \leq \sum_{i=1}^{1+r_K} |Q_i| - |G| \cdot r_K \leq (d_1 \cdot |G| + (1 + r_K - d_1)|G|/p) - r_K|G|$$
$$= (d_1 - r_K)|G|(1 - 1/p) + |G|/p.$$

It is clear that this inequality implies that $d_1 \geq r_K$, and hence that $d - d_1 \leq 1$, which proves claim (ii).

To prove claim (iii) we note that if $\delta_L = 0$, then claim (ii) implies that

$$1 + |G| \cdot r_K = 1 + r_L = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot A_L^{\Sigma}) = |G| \cdot r_K + |G/J|$$

with J equal to either $\{\varepsilon\}$ (if $n_{\{\varepsilon\}} > |G|$) or to H' (if $n_{\{\varepsilon\}} = |G|$) and hence that both $n_{\{\varepsilon\}} = |G|$ and $H' = G$, as claimed.

This completes the proof of Corollary 4.1.3.

4.4 The proof of Corollary 4.1.7

We fix a cyclic group G of order p^n and for each integer i with $1 \leq i \leq n$ write G_i for the subgroup of G of order p^i.

If the inequality (4.3) is true, it implies that the non-negative integer $m_I(F/E)$ can be non-zero for only finitely many modules I in $\mathrm{IM}_{p,n}$. This implies that only finitely many isomorphism classes of indecomposable $\mathbb{Z}_p[G]$-lattices can occur as direct summands of $\overline{A_L^p}$ as L/K runs over the indicated class of extensions and so the final assertion of Corollary 4.1.7 would be true.

It is therefore enough to prove the inequality (4.3).

For any natural number d and each indecomposable lattice I in $\mathrm{IM}_{p,n}$ we write $\widetilde{m}_I^d$ for the maximal multiplicity with which I occurs as a direct summand of any $\mathbb{Z}_p[\Gamma]$-lattice N for which one has $\mathrm{rk}_p(\hat{H}^{-1}(\Gamma_i, N)) \leq d$ for all integers i with $1 \leq i \leq n$.

Then the key point in the proof of (4.3) is that Burns [9, Lemma 3.2] has combined Theorem 4.2.1 with a careful analysis of the diagrams (4.4) to show that

$$\sum_{I \in \mathrm{IM}_{p,n}} \widetilde{m}_I^d \leq p^{n(n-1)d^2} \cdot \kappa_n^d \tag{4.6}$$

where κ_n^d is the integer defined just prior to the statement of Corollary 4.1.7.

Remark 4.4.1. Macias Castillo has recently used a finer analysis of the diagrams (4.4) to show that in special cases the bound given by (4.6) can be significantly improved (for details see [30]). By substituting the bound obtained by Macias Castillo in place of (4.6) we would obtain a corresponding improvement of Corollary 4.1.7.

The inequality (4.6) implies that the required inequality (4.3) will be true if we can show the existence, under the stated conditions, of an integer d that depends only on F/E and is such that $\mathrm{rk}_p(\hat{H}^{-1}(\mathrm{Gal}(L/K), \overline{A_L^p})) \leq d$ for all cyclic extensions L/K of degree at most p^n and with $E \subseteq K \subset L \subset F$ and K/E finite.

But Lemma 4.2.4(i) gives an isomorphism of groups

$$\hat{H}^{-1}(\mathrm{Gal}(L/K), \overline{A_L^p}) \cong T_{L/K}^p = \mathrm{coker}\left(\mathrm{Gal}(M_L^p/L)_{\mathrm{tor}} \xrightarrow{\pi_{L/K}} \mathrm{Gal}(M_K^p/L)_{\mathrm{tor}}\right)$$

and so it will be enough to show that the stated conditions imply the existence of an integer d that depends only on F/E and is such that

$$\mathrm{rk}_p(A_{L,\mathrm{tor}}^p) \leq d$$

for all finite extensions L of E in F.

We now use the following formula proved by Gras in [19, Theorem 12]:

$$\mathrm{rk}_p(A^p_{L,\mathrm{tor}}) = g(L) - \nu(L) + \mathrm{rk}_p(\mathrm{Cl}'_{L(\zeta_p)}) - \delta_L. \tag{4.7}$$

In this formula $g(L)$ is the number of p-adic places in L, $\nu(L)$ is either 0 or 1 (depending on whether or not L contains ζ_p) and $\mathrm{Cl}'_{L(\zeta_p)}$ is a certain subquotient of the ideal class group $\mathrm{Cl}_{L(\zeta_p)}$ of the field $L(\zeta_p)$.

Since all p-adic places of E are assumed to have an open decomposition group in $\mathrm{Gal}(E_\infty/E)$, there are only finitely many p-adic places in E_∞ and so $g(L)$ is bounded above by a value that depends only on F/E. Gras' formula therefore means it is enough to show that the same is true for $\mathrm{rk}_p(\mathrm{Cl}_{L(\zeta_p)})$.

For any extension E' of E we write $X_{E'}$ for the Galois group of the maximal unramified abelian pro-p extension of E' in $\mathbb{Q}^c$.

Note that for any L as above the compositum of $L(\zeta_p)$ and E_∞ is an intermediate field of $F(\zeta_p)/E_\infty(\zeta_p)$ that is a $\mathbb{Z}_p$-extension of $L(\zeta_p)$. Since there are only finitely many intermediate fields of the finite extension $F(\zeta_p)/E_\infty(\zeta_p)$ a standard argument of Iwasawa theory (as discussed, for example, by Washington in [38, Proposition 13.23]) that relies on the structure theory of finitely generated torsion Iwasawa modules implies that it will be enough for us to show that, for each such intermediate field D, the $\mathbb{Z}_p$-module X_D is finitely generated.

Now each such field D is a finite Galois extension of $E_\infty(\zeta_p)$ of p-power degree and so the structure theory of finte groups of p-power order implies that we can choose a finite chain of subgroups

$$\mathrm{Gal}(F(\zeta_p)/D) = J_0 \trianglelefteq J_1 \trianglelefteq \cdots \trianglelefteq J_n = \mathrm{Gal}(F(\zeta_p)/E_\infty(\zeta_p))$$

with $|J_{i+1}/J_i| = p$ for all i with $0 \le i \le n$.

We set $D_i := D^{J_i}$ for each such i so that $D_0 = D, D_n = E_\infty(\zeta_p)$ and each extension

D_i/D_{i+1} is Galois of degree p.

By assumption, the Iwasawa μ-invariant of $E_\infty(\zeta_p)/E(\zeta_p)$ vanishes and so the $\mathbb{Z}_p$-module $X_{D_n} = X_{E_\infty(\zeta_p)}$ is finitely generated. In addition, since E_∞ has finitely many p-adic places the same is true for $F(\zeta_p)$ and so for each i with $0 \le i \le n$, the field D_i has finitely many p-adic places.

To prove that the $\mathbb{Z}_p$-module X_D is finitely generated we can therefore apply the result of Lemma 4.4.2 below successively to each of the extensions D_i/D_{i+1}, starting from $i = n-1$ and descending to $i = 0$.

This completes the proof of the inequality (4.3) and hence also of Corollary 4.1.7.

Lemma 4.4.2. Let D be a subfield of $\mathbb{Q}^c$ with only finitely many p-adic places and such that the $\mathbb{Z}_p$-module X_D is finitely generated. Then for any Galois extension D' of D of degree p the $\mathbb{Z}_p$-module $X_{D'}$ is also finitely generated.

Proof. Write $M_{D'}$ and M_D for the maximal unramified abelian pro-p extensions of D' and D and set $\Delta := \mathrm{Gal}(D'/D)$.

Then the maximality condition on $M_{D'}$ implies that it is Galois over D and, since D'/D is cyclic, the group of coinvariants $H_0(\Delta, X_{D'})$ identifies with $\mathrm{Gal}(M/D')$ where M is the maximal abelian extension of D in $M_{D'}$.

The inertia degree in M/D of each of the finitely many p-adic places of D is at most p and so the subgroup I of $\mathrm{Gal}(M/D)$ that is generated by the inertia subgroups of these places is finite. In addition, the fixed field M^I is a subfield of M_D and so $(\mathrm{Gal}(M/D))/I \cong \mathrm{Gal}(M^I/D)$ is isomorphic to a quotient of the finitely generated $\mathbb{Z}_p$-module X_D. Since I is finite, this shows that the $\mathbb{Z}_p$-module $\mathrm{Gal}(M/D)$, and hence also its submodule

$$\mathrm{Gal}(M/D') = H_0(\Delta, X_{D'}) = X_{D'}/I_\Delta(X_{D'}),$$

where $I_\Delta(X_{D'})$ is the augumentation ideal of $\mathbb{Z}_p[\Delta]$, is finitely generated.

Since I_Δ is contained in the Jacobson Radical of $\mathbb{Z}_p[\Delta]$, Nakayama's Lemma implies that $X_{D'}$ is finitely generated over $\mathbb{Z}_p[\Delta]$, and hence (since Δ is finite) also over $\mathbb{Z}_p$. $\square$

4.5 The vanishing of $T^{\Sigma}_{L/K}$

Motivated by the results of Theorem 4.1.1 and Corollary 4.1.3 we now end this chapter by providing a useful characterisation of the vanishing of groups $T^{\Sigma}_{L/K}$.

We start by recalling an important class of field extensions.

Definition 4.5.1. An extension of number fields L/K is said to be '$\mathbb{Z}_p$-extendable' if there exists a Galois extension L' of K in $\mathbb{Q}^c$ that contains L and is such that $\mathrm{Gal}(L'/K)$ is topologically isomorphic to $\mathbb{Z}_p$.

Remark 4.5.2. Extensions that are $\mathbb{Z}_p$-extendable have been extensively investigated in the literature, and by a variety of authors. For recent results in this direction see, for example, Seo [36].

Remark 4.5.3. We can describe what it means for an extension L of K to be $\mathbb{Z}_p$-extendable in terms of the torsion subgroup of A^{Σ}_K.

Writing A^{Σ}_K as

$$A^{\Sigma}_K \cong (A^{\Sigma}_K)_{\mathrm{tor}} \times \mathbb{Z}_p^{d_K}$$

for some $d_K \in \mathbb{N}$, take the fixed field of M^{Σ}_K by $A^{\Sigma}_{K,\mathrm{tor}}$ and call this field $M^{\Sigma}_{K,\mathbb{Z}_p}$. An extension L of K being $\mathbb{Z}_p$-extendable is equivalent to saying that L is contained in $M^{\Sigma}_{K,\mathbb{Z}_p}$. This is true if and only if $(A^{\Sigma}_K)_{\mathrm{tor}}$ acts trivially on L, or equivalently if the map

$$A^{\Sigma}_{K,\mathrm{tor}} \hookrightarrow A^{\Sigma}_K \to \mathrm{Gal}(L/K)$$

is the zero map.

It is clear that A_K^Σ is torsion-free if and only if all cyclic degree p extensions of K that are unramified outside Σ are $\mathbb{Z}_p$-extendable.

In addition, it is also clear that for any finite set of places Σ of K that contains all p-adic places the group A_K^Σ is torsion-free if and only if all cyclic degree p extensions of K that are unramified outside Σ are $\mathbb{Z}_p$-extendable.

In the following result we use the concept of $\mathbb{Z}_p$-extendability to give a useful criterion for the vanishing of the groups $T_{L/K}^\Sigma$.

For a number field E we write $E^{\max}$ for the maximal $\mathbb{Z}_p$-power extension of E inside $\mathbb{Q}^c$.

Lemma 4.5.4. Assume that L/K is cyclic of finite p-power degree and unramified outside a finite set of places Σ that contains all p-adic places.

(i) $T_{L/K}^\Sigma$ is naturally isomorphic to the torsion subgroup of $\mathrm{Gal}((L^{\max} \cap M_K^\Sigma)/L)$.

(ii) The following conditions are equivalent:

  (a) $T_{L/K}^\Sigma$ vanishes.

  (b) For any degree p extension F of L that is abelian over K one has

$$\begin{aligned} &F/L \text{ is } \mathbb{Z}_p\text{-extendable} \\ &\qquad \iff F \text{ is contained in a } \mathbb{Z}_p\text{-extension of } L \text{ that is abelian over } K. \end{aligned}$$

(iii) If L/K is $\mathbb{Z}_p$-extendable, then $T_{L/K}^\Sigma$ is equal to the cokernel of the restriction map $A_{L,\mathrm{tor}}^\Sigma \to A_{K,\mathrm{tor}}^\Sigma$. In this case the following conditions are equivalent:

  (a) $T_{L/K}^\Sigma$ vanishes.

  (b) $L^{\max} \cap M_K^\Sigma = K^{\max}$.

(c) For any degree p Galois extension K' of K in M_K^Σ that is not $\mathbb{Z}_p$-extendable the extension LK'/L is not $\mathbb{Z}_p$-extendable.

Proof. Recall that $T_{L/K}^\Sigma$ is the cokernel of the map

$$\mathrm{Gal}(M_L^\Sigma/L)_{\mathrm{tor}} \to \mathrm{Gal}(M_K^\Sigma/L)_{\mathrm{tor}}.$$

To prove claim (i) we note $A_{L,\mathrm{tor}}^\Sigma = \mathrm{Gal}(M_L^\Sigma/L^{\max})$ and that $\mathrm{Gal}(M_K^\Sigma/L)_{\mathrm{tor}} = \mathrm{Gal}(M_K^\Sigma/E)$ with E a subfield of $L^{\max}$ such that E/L is $\mathbb{Z}_p$-free and $(M_K^\Sigma \cap L^{\max})/E$ is finite. Therefore the claimed isomorphism follows from the fact that the image of $\mathrm{Gal}(M_L^\Sigma/L^{\max})$ under the restriction map $\mathrm{Gal}(M_L^\Sigma/L) \to \mathrm{Gal}(M_K^\Sigma/L)$ is $\mathrm{Gal}(M_K^\Sigma/(M_K^\Sigma \cap L^{\max}))$.

Set $E^* := M_K^\Sigma \cap L^{\max}$. Then claim (i) implies that $T_{L/K}^\Sigma$ vanishes if and only if $\mathrm{Gal}(E^*/L)$ is $\mathbb{Z}_p$-free. The latter condition is satisfied if and only if every intermediate field of E^*/L of degree p over L is contained in an intermediate field that is a $\mathbb{Z}_p$-extension of L and hence is equivalent to the condition in claim (ii)(b).

The first assertion of claim (iii) is true because if L/K is $\mathbb{Z}_p$-extendable, then $L \subseteq K^{\max}$ and so $\mathrm{Gal}(M_K^\Sigma/L)_{\mathrm{tor}} = \mathrm{Gal}(M_K^\Sigma/K^{\max}) = A_{K,\mathrm{tor}}^\Sigma$.

In this case therefore the group $T_{L/K}^\Sigma$ vanishes if and only if the natural restriction map $A_{L,\mathrm{tor}}^\Sigma \to A_{K,\mathrm{tor}}^\Sigma$ is surjective, or equivalently $L^{\max} \cap M_K^\Sigma = K^{\max}$. This shows the equivalence of (iii)(a) and (iii)(b).

For the equivalence of (iii)(a) and (iii)(c), first assume that $T_{L/K}^\Sigma$ vanishes and let K' be an extension of K which is not $\mathbb{Z}_p$-extendable. By Remark 4.5.3 above, this means that the map $A_{K,\mathrm{tor}}^\Sigma \to \mathrm{Gal}(K'/K)$ is not the zero map. We would like to show that the extension LK'/K is also not $\mathbb{Z}_p$-extendable.

Suppose that LK'/K is $\mathbb{Z}_p$-extendable. Then, since $L \subseteq LK'$, the extension LK'/L is also $\mathbb{Z}_p$-extendable and the map $A_{L,\mathrm{tor}}^\Sigma \to \mathrm{Gal}(LK'/K)$ is the zero map, and we have a commutative diagram:

$$\begin{tikzcd}
(A_L^\Sigma)_{\mathrm{tor}} \arrow[r] \arrow[d] & \mathrm{Gal}(LK'/L) \arrow[d] \\
(A_K^\Sigma)_{\mathrm{tor}} \arrow[r] & \mathrm{Gal}(K'/K).
\end{tikzcd}$$

Since $T_{L/K}^\Sigma$ vanishes, the map $A_{L,\mathrm{tor}}^\Sigma \to A_{K,\mathrm{tor}}^\Sigma$ is surjective. This implies that the bottom map $A_{K,\mathrm{tor}}^\Sigma \to \mathrm{Gal}(K'/K)$ is also the zero map, which is a contradiction.

Conversely, assume that $T_{L/K}^\Sigma$ does not vanish, i.e. that the restriction map $A_{L,\mathrm{tor}}^\Sigma \to A_{K,\mathrm{tor}}^\Sigma$ is not surjective. Then by Nakayama's Lemma, the map $\pi_p : A_{L,\mathrm{tor}}^\Sigma \to (A_{K,\mathrm{tor}}^\Sigma)/p$ is also not surjective.

Next, we write $A_K^\Sigma \cong A_{K,\mathrm{tor}}^\Sigma \times \Delta$ where $\Delta \cong \mathbb{Z}_p^{d_K}$ for some $d_K \in \mathbb{N}$. Take the fixed field of M_K^Σ by Δ, and call this field K'. Then $\mathrm{Gal}(K'/K) \cong A_{K,\mathrm{tor}}^\Sigma$ and the extension K'/K is not $\mathbb{Z}_p$-extendable.

Let $K^{(p)}$ denote the maximal extension of K in K' with Galois group of exponent p. Then $A_{K,\mathrm{tor}}^\Sigma/p \cong \mathrm{Gal}(K^{(p)}/K)$. Take E to be the subextension of $K^{(p)}$ such that $\mathrm{Gal}(E/K) \cong (A_{K,\mathrm{tor}}^\Sigma/p)/\mathrm{Im}(\pi_p)$, and F the subextension of E such that $[F : K] = p$ (note that $E \neq K$ because π_p is not surjective). Then we have:

- $A_{K,\mathrm{tor}}^\Sigma$ does not act trivially on F by construction, and
- $A_{L,\mathrm{tor}}^\Sigma$ acts trivially on F by the definition of E.

Therefore $A_{L,\mathrm{tor}}^\Sigma$ must act trivially on the compositum LF, hence LF/L is $\mathbb{Z}_p$-extendable. However, since $A_{K,\mathrm{tor}}^\Sigma$ does not act trivially on F, the extension F/K is not $\mathbb{Z}_p$-extendable. We have now shown that if $T_{L/K}^\Sigma$ is not zero, then there exists an extension F of K of degree p which is not $\mathbb{Z}_p$-extendable, but such that LF/L is $\mathbb{Z}_p$-extendable.

$\square$

Chapter 5

Ray class groups over cyclic extensions of small degree

We recall that if G is a cyclic group of order p^n, then a complete classification of the isomorphism classes of indecomposable $\mathbb{Z}_p[G]$-lattices is (only) known if $n \leq 2$.

In this chapter we will use these classifications, due to Diederichsen [15] in the case $n = 1$ and to Heller and Reiner [20] in the case $n = 2$, to investigate much more explicitly the Galois structures of the groups A_L^Σ and B_L^Σ.

In the case $n = 1$ the result that we obtain is complete and gives a different proof of an earlier observation of Burns and Macias Castillo from [12, Corollary 5.5].

However, in the case $n = 2$ the classification result of Heller and Reiner is much more complicated and we achieve only partial success.

The overall approach of this chapter is heavily influenced by the extensive earlier work of Rzedowski-Calderón, Villa Salvador and Madan [35] and of Elder and Madan [16, 17] concerning the Galois structure of valuation rings in wildly ramified Galois extensions of p-adic fields.

We assume throughout this chapter that Leopoldt's Conjecture is valid at p.

5.1 The case $|G| = p$

In this section we fix a Galois extension of number fields L/K of degree p and set $G := \mathrm{Gal}(L/K)$. We also fix a finite set of places of K that contains all archimedean places, all that ramify in L/K and all that divide p.

In this case there are three isomorphism classes of indecomposable $\mathbb{Z}_p[G]$-lattices and there basic properties are given by the following table (taken from [35]) in which we write Tr_G for the element $\sum_{g\in G} g$ of $\mathbb{Z}_p[G]$.

Table I

M	$H^0(G,M)$	$\hat{H}^{-1}(G,M)$	$\mathrm{rk}_{\mathbb{Z}_p}(M)$
$\mathbb{Z}_p[G]$	$\mathbb{Z}_p$	0	p
$\mathcal{O}_p := \mathbb{Z}_p[G]/\mathrm{Tr}_G$	0	$\mathbb{Z}/p\,\mathbb{Z}$	$p-1$
$\mathbb{Z}_p$	$\mathbb{Z}_p$	0	1

By using this classification, the following result gives a complete description of the Galois structure of the $\mathbb{Z}_p[G]$-lattice $\overline{A_L^\Sigma}$ in terms of the finite group $T^\Sigma_{L/K}$ defined at the beginning of Chapter 4.

Proposition 5.1.1. Let p be an odd prime, assume that Leopoldt's Conjecture is valid for L at p and set $d := \dim_{\mathbb{F}_p}(T^\Sigma_{L/K})$. Then there is an isomorphism of $\mathbb{Z}_p[G]$-modules

$$\overline{A_L^\Sigma} \cong \mathbb{Z}_p[G]^{r_K-d} \oplus \mathcal{O}_p^d \oplus \mathbb{Z}_p^{d+1}.$$

Proof. The Krull-Schmidt theorem combines with Table I to imply that for suitable non-negative integers a, b and c there is an isomorphism of $\mathbb{Z}_p[G]$-modules

$$\overline{A_L^\Sigma} \cong \mathbb{Z}_p[G]^a \oplus \mathcal{O}_p^b \oplus \mathbb{Z}_p^c. \tag{5.1}$$

We therefore need to show that the integers a, b and c are uniquely determined by the integer d.

To see this we use the decomposition (5.1) in conjunction with the fourth column of Table I to compute

$$\mathrm{rk}_{\mathbb{Z}_p}(\overline{A_L^\Sigma}) = ap + b(p-1) + c \tag{5.2}$$

and in conjunction with the second column of Table I also

$$\mathrm{rk}_{\mathbb{Z}_p}(H^0(G, \overline{A_L^\Sigma})) = \mathrm{rk}_{\mathbb{Z}_p}(\mathbb{Z}_p^a \oplus 0 \oplus \mathbb{Z}_p^c) = a + c. \tag{5.3}$$

Now since Leopoldt's Conjecture is assumed to be valid for L (and hence also for K) at p, and L/K has degree p (so $r_L = p \cdot r_K$), the equality (4.1) implies that

$$\mathrm{rk}_{\mathbb{Z}_p}(\overline{A_L^\Sigma}) = r_L + 1 = p \cdot r_K + 1 \tag{5.4}$$

and also

$$\mathrm{rk}_{\mathbb{Z}_p}(H^0(G, \overline{A_L^\Sigma})) = \mathrm{rk}_{\mathbb{Z}_p}(\overline{A_K^\Sigma}) = r_K + 1 \tag{5.5}$$

where the first equality follows from Lemma 3.3.2(i).

By comparing the results of subtracting (5.3) from (5.2), and subtracting (5.5) from (5.4), one finds that $a = r_K - b$ and by using this to compare (5.3) with (5.5) we find that $c = b + 1$.

We now note that Lemma 4.2.4(i) implies that the group $\hat{H}^{-1}(G, \overline{A_L^\Sigma})$ is isomorphic to $T_{L/K}^\Sigma$. Since the third column of Table I combines with the isomorphism (5.1) to imply that

$\hat{H}^{-1}(G, \overline{A_L^\Sigma})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^b$ we deduce that

$$b = \dim_{\mathbb{F}_p}((\mathbb{Z}/p\mathbb{Z})^b) = \dim_{\mathbb{F}_p}(\hat{H}^{-1}(G, \overline{A_L^\Sigma})) = \dim_{\mathbb{F}_p}(T_{L/K}^\Sigma)$$

which, by definition, is equal to d.

Putting everything together we find that $a = r_K - d$ and $c = d + 1$, as claimed. $\square$

5.2 The case $|G| = p^2$

In this section we fix a Galois extension of number fields L/K of degree p^2, with $G := \mathrm{Gal}(L/K)$ and also a finite set of places Σ of K that contains all archimedean places, all places above p and all that ramify in L/K.

We write F for the (unique) intermediate field of L/K with $[L : F] = p$ and set $H := \mathrm{Gal}(L/F)$. We also set $r := r_K$ and note that $r_L = p^2 \cdot r_K$.

In this case, Heller and Reiner [20] have shown that there are $4p+1$ isomorphism classes of indecomposable $\mathbb{Z}_p[G]$-lattices. The basic properties of these lattices are conveniently recorded in Table II given below (and taken from [20, Table 2]).

In this table we write R_1 and R_2 for the modules $\frac{\mathbb{Z}_p[x]}{(\Phi_p(x))}$ and $\frac{\mathbb{Z}_p[x]}{(\Phi_{p^2}(x))}$, where $\Phi_{p^i}(x)$ is the $p^{i-\mathrm{th}}$ cyclotomic polynomial, and in each case a fixed generator of G acts on the quotient as multiplication by x.

For a $\mathbb{Z}_p[G/H]$-lattice X the notation $(R_2, X; \lambda_0^i)$ denotes a module that arises as the extension of R_2 by X that corresponds to the i-th power of a certain element λ_0 of $\mathrm{Ext}^1_{\mathbb{Z}_p[G]}(R_2, X) \cong X/pX$.

Remark 5.2.1. The indecomposable $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p[G]$ has $\mathbb{Z}_p$-rank equal to p^2 and is a cohomologically trivial G-module. This implies that $(R_2, E; 1)$ is isomorphic to $\mathbb{Z}_p[G]$ as it is the only module in Table II which satisfies both $\mathrm{rk}_{\mathbb{Z}_p}(M) = p^2$ and $\hat{H}^{-1}(G, M) = 0$.

Table II

M	M/H	$H^0(H,M)$	$H^0(G,M)$	$\hat{H}^{-1}(G,M)$	$\mathrm{rk}_{\mathbb{Z}_p}(M)$
R_2	$\mathcal{O}_p^p$	0	0	C_p	$p(p-1)$
R_1	$\mathbb{Z}_p^{p-1}$	R_1	0	C_p	$p-1$
$\mathbb{Z}_p$	$\mathbb{Z}_p$	$\mathbb{Z}_p$	$\mathbb{Z}_p$	0	1
$E \cong \mathbb{Z}_p[G/H]$	$\mathbb{Z}_p^p$	E	$\mathbb{Z}_p$	0	p
$(R_2, Z; 1)$	$\mathbb{Z}_p[H] \oplus \mathcal{O}_p^{p-1}$	$\mathbb{Z}_p$	$\mathbb{Z}_p$	0	$1+p(p-1)$
$(R_2, R_1; \lambda_0^i)$	$\mathbb{Z}_p[H]^{p-i-1} \oplus \mathcal{O}_p^{i+1} \oplus \mathbb{Z}_p^i$	R_1	0	$C_{p^2}, i=0$	p^2-1
$0 \leq i \leq p-2$				$C_p \oplus C_p, i>0$	
$(R_2, E; \lambda_0^i)$	$\mathbb{Z}_p[H]^{p-i} \oplus \mathcal{O}_p^i \oplus \mathbb{Z}_p^i$	E	$\mathbb{Z}_p$	$0, i=0$	p^2
$0 \leq i \leq p-1$				$C_p, i>0$	
$(R_2, \mathbb{Z}_p \oplus R_1; 1 \oplus \lambda_o^i)$	$\mathbb{Z}_p[H]^{p-i-1} \oplus \mathcal{O}_p^{i+1} \oplus \mathbb{Z}_p^{i+1}$	$\mathbb{Z}_p \oplus R_1$	$\mathbb{Z}_p$	C_p	p^2
$0 \leq i \leq p-2$					
$(R_2, \mathbb{Z}_p \oplus E; 1 \oplus \lambda_0^i)$	$\mathbb{Z}_p[H]^{p-i} \oplus \mathcal{O}_p^i \oplus \mathbb{Z}_p^{i+1}$	$\mathbb{Z}_p \oplus E$	$\mathbb{Z}_p \oplus \mathbb{Z}_p$	0	p^2+1
$1 \leq i \leq p-2$					

5.2.1 The case $T^{\Sigma}_{L/F} = 0$

Proposition 5.2.2. Assume that $T^{\Sigma}_{L/F} = 0$ and that Leopoldt's Conjecture is valid for L at p. Then there is an isomorphism of $\mathbb{Z}_p[G]$-modules $\overline{A^{\Sigma}_L} \cong \mathbb{Z}_p[G]^r \oplus \mathbb{Z}_p$.

Proof. We first consider $\overline{A^{\Sigma}_L}$ as a $\mathbb{Z}_p[H]$-module. Then the argument in §5.1 implies that there are (unique) non-negative integers α, β and γ for which there is an isomorphism of $\mathbb{Z}_p[H]$-modules of the form

$$\overline{A^{\Sigma}_L} \cong \mathbb{Z}_p[H]^{\alpha} \oplus \mathcal{O}_p^{\beta} \oplus \mathbb{Z}_p^{\delta}$$

Since Lemma 4.2.4(i) implies that $T^{\Sigma}_{L/F}$ is isomorphic to $\hat{H}^{-1}(H, \overline{A^{\Sigma}_L})$, we find that the assumption $T^{\Sigma}_{L/F} = 0$ implies (via the third column of Table I) that $\beta = 0$.

Since the second column in Table II shows that the only indecomposable $\mathbb{Z}_p[G]$-lattices which, when considered as $\mathbb{Z}_p[H]$-modules, do not contain a direct summand that is isomorphic to $\mathcal{O}_p$ are $R_1, \mathbb{Z}_p, E$ and $(R_2, E; 1)$, it follows that there must exist non-negative integers a, b, c, d for which there is an isomorphism of $\mathbb{Z}_p[G]$-modules of the form

$$\overline{A^{\Sigma}_L} \cong R_1^a \oplus Z^b \oplus E^c \oplus (R_2, E; 1)^d. \tag{5.6}$$

We combine this decomposition with the data given in Table II, the result of Lemma 3.3.2(i) and the assumed validity of Leopoldt's Conjecture at p to compute that

$$\begin{aligned} \mathrm{rk}_{\mathbb{Z}_p}(\overline{A^{\Sigma}_L}) &= a(p-1) + b + cp + dp^2 = p^2 r + 1 \\ \mathrm{rk}_{\mathbb{Z}_p}(H^0(H, \overline{A^{\Sigma}_L})) &= a(p-1) + b + cp + dp = pr + 1 \\ \mathrm{rk}_{\mathbb{Z}_p}(H^0(G, \overline{A^{\Sigma}_L})) &= b + c + d = r + 1. \end{aligned}$$

Comparing these equalities one finds that $a = c = 0$, $b = 1$ and $d = r$. Therefore, after recalling Remark 5.2.1, we obtain the claimed result as a consequence of (5.6). □

5.2.2 The case $T^{\Sigma}_{L/F} \neq 0$ and $T^{\Sigma}_{L/K} = 0$

Proposition 5.2.3. Assume that $T^{\Sigma}_{L/F} \neq 0$ and $T^{\Sigma}_{L/K} = 0$ and that Leopoldt's Conjecture is valid for L at p. Then one of the following two cases occurs.

(i) $|T^{\Sigma}_{L/F}| = p^{p-1}$ and there is an isomorphism $\overline{A^{\Sigma}_{L}} \cong (R_2, \mathbb{Z}_p; 1) \oplus E \oplus \mathbb{Z}_p[G]^{r-1}$ of $\mathbb{Z}_p[G]$-modules.

(ii) $|T^{\Sigma}_{L/F}| = p^i$ for some integer i with $1 \leq i \leq p-2$ and there is an isomorphism of $\mathbb{Z}_p[G]$-modules $\overline{A^{\Sigma}_{L}} \cong (R_2, \mathbb{Z}_p \oplus E; 1 \oplus \lambda_0^i) \oplus \mathbb{Z}_p[G]^{r-1}$.

Proof. Firstly, the fifth column of Table II implies that the only indecomposable $\mathbb{Z}_p[G]$-lattices M for which the group $\hat{H}^{-1}(G, M)$ vanishes are $\mathbb{Z}_p, E, (R_2, \mathbb{Z}_p; 1), (R_2, E; 1)$ and $(R_2, \mathbb{Z}_p \oplus E; 1 \oplus \lambda_0^i)$ for any choice of i with $1 \leq i \leq p-2$.

Of these lattices, the only ones that also satisfy $\hat{H}^{-1}(H, M) \neq 0$ are

$$J := (R_2, \mathbb{Z}_p; 1) \quad \text{and} \quad J_i := (R_2, \mathbb{Z}_p \oplus E; 1 \oplus \lambda_0^i)$$

for some choice of i with $1 \leq i \leq p-2$.

Lemma 4.2.4(i) therefore implies that at least one of the modules J or J_i must appear in the Krull-Schmidt decomposition of $\overline{A^{\Sigma}_{L}}$ and that all other summands must be from the list of modules given above.

We can therefore consider two separate cases that, taken together, exhaust all possibilities.

Case 1: $\overline{A^{\Sigma}_{L}}$ contains no direct summand that is isomorphic to a module J_i.

In this case, some direct summand of $\overline{A^{\Sigma}_{L}}$ must be isomorphic to J and so there is an isomorphism of $\mathbb{Z}_p[G]$-modules of the form

$$\overline{A^{\Sigma}_{L}} \cong J^a \oplus \mathbb{Z}_p^b \oplus E^c \oplus (R_2, E; 1)^d$$

for suitable non-negative integers a, b, c and d and with $a > 0$.

Using Table II, Lemma 3.3.2(i) and the assumed validity of Leopoldt we now compute

$$\begin{aligned}
\mathrm{rk}_{\mathbb{Z}_p}(\overline{A_L^\Sigma}) &= a(1+p(p-1)) + b + cp + dp^2 = p^2 r + 1\\
\mathrm{rk}_{\mathbb{Z}_p}(H^0(H, \overline{A_L^\Sigma})) &= a + b + cp + dp = pr + 1\\
\mathrm{rk}_{\mathbb{Z}_p}(H^0(G, \overline{A_L^\Sigma})) &= a + b + c + d = r + 1.
\end{aligned}$$

Comparing these equalities we find that $c + d = r$ and $a + b = 1$. Hence, since $a > 0$ we must have $a = 1$ and $b = 0$ and hence also $c = 1$ and $d = r - 1$. This gives the isomorphism described in (i) and by combining the second column of Table II with the fourth column of Table I we compute that

$$|T_{L/F}^\Sigma| = |\hat{H}^{-1}(H, \overline{A_L^\Sigma})| = |(\mathbb{Z}/p\,\mathbb{Z})^{p-1}| = p^{p-1},$$

as claimed.

Case 2: $\overline{A_L^\Sigma}$ contains a direct summand that is isomorphic to some module J_i.

Write a for the number of direct summands that are isomorphic to any of the modules J_i and write these modules as M_i for $1 \le i \le a$. Then there is an isomorphism of $\mathbb{Z}_p[G]$-modules

$$\overline{A_L^\Sigma} \cong \bigoplus_{i=1}^{a} M_i \oplus J^b \oplus \mathbb{Z}_p^c \oplus E^d \oplus (R_2, E; 1)^e$$

for non-negative integers b, c, d and e.

Just as above, we combine this isomorphism with Table II to compute

$$
\begin{aligned}
\mathrm{rk}_{\mathbb{Z}_p}(\overline{A_L^{\Sigma}}) &= a(p^2+1) + b(a + p(p-1)) + c + dp + ep^2 = p^2 r + 1 \\
\mathrm{rk}_{\mathbb{Z}_p}(H^0(H, \overline{A_L^{\Sigma}})) &= a(1+p) + b + c + dp + ep = pr + 1 \\
\mathrm{rk}_{\mathbb{Z}_p}(H^0(G, \overline{A_L^{\Sigma}})) &= 2a + b + c + d + e = r + 1.
\end{aligned}
$$

By comparing these equations we find that $a = 1, b = c = 0, d = 0$ and $e = r - 1$. This implies the existence of a unique integer i_* with $1 \leq i_* \leq p-2$ for which there is an isomorphism of $\mathbb{Z}_p[G]$-modules

$$
\overline{A_L^{\Sigma}} \cong J_{i_*} \oplus (R_2, E; 1)^{r-1} \cong (R_2, \mathbb{Z}_p \oplus E; 1 \oplus \lambda_0^{i_*}) \oplus \mathbb{Z}_p[G]^{r-1}.
$$

We then combine the isomorphism of Lemma 4.2.4(i) with the second column of Table II to compute

$$
|T_{L/F}^{\Sigma}| = |\hat{H}^{-1}(H, \overline{A_L^{\Sigma}})| = |(\mathbb{Z}/p\,\mathbb{Z})^{i_*}| = p^{i_*}
$$

as claimed in (ii). $\square$

5.2.3 The case $T_{L/F}^{\Sigma} \neq 0$ and $T_{L/K}^{\Sigma} \neq 0$

This is the most difficult case and our results are only very partial.

Note that this case implies that $r > 0$ since otherwise $\overline{A_L^{\Sigma}}$ must be isomorphic to $\mathbb{Z}_p$ and so Lemma 4.2.4(i) implies that $T_{L/F}^{\Sigma}$ and $T_{L/K}^{\Sigma}$ vanish. We therefore consider the simplest possible case, where $r = 1$.

In addition, the description of Lemma 4.2.4(i) implies that $T_{L/K}^{\Sigma}$ has exponent either p or p^2 and we use this fact to split the discussion into two separate cases.

Proposition 5.2.4. Assume that $r = 1$, that $T_{L/K}^{\Sigma}$ has exponent p^2, that $T_{L/K}^{\Sigma}$ does not vanish and that Leopoldt's Conjecture is valid for L at p.

Then one has $|T^{\Sigma}_{L/K}| = p^2$ and $|T^{\Sigma}_{L/F}| = p$ and there is an isomorphism of $\mathbb{Z}_p[G]$-modules $\overline{A^{\Sigma}_L} \cong (R_2, R_1; 1) \oplus \mathbb{Z}_p^2$.

Proof. Table II implies that there is an isomorphism of $\mathbb{Z}_p[G]$-modules of the form

$$\begin{aligned}\overline{A^{\Sigma}_L} \cong R_2^a \oplus R_1^b \oplus \mathbb{Z}_p^c \oplus E^d \oplus (R_2, \mathbb{Z}_p; 1)^e \oplus \sum_{i=0}^{p-2} (R_2, R_1; \lambda_0^i)^{f_i} \\ \oplus \sum_{i=0}^{p-1} (R_2, E; \lambda_0^i)^{g_i} \oplus \sum_{i=0}^{p-2} (R_2, \mathbb{Z}_p \oplus R_1; 1 \oplus \lambda_0^i)^{h_i} \oplus \sum_{i=1}^{p-2} (R_2, \mathbb{Z}_p \oplus E; 1 \oplus \lambda_0^i)^{j_i}\end{aligned}$$

where $a, b, c, d, e, f_i, g_i, h_i, j_i$ are suitable non-negative integers.

Then, by using the fifth column of Table II, one checks that $\hat{H}^{-1}(G, \overline{A^{\Sigma}_L})$ is isomorphic to $(\mathbb{Z}/p\,\mathbb{Z})^{\alpha} \oplus (\mathbb{Z}/p^2\,\mathbb{Z})^{\beta}$ with

$$\alpha := a + b + \sum_{i=1}^{p-2} 2f_i + \sum_{i=1}^{p-1} g_i + \sum_{i=0}^{p-2} h_i \quad \text{and} \quad \beta := f_0,$$

and hence that $f_0 > 0$.

In addition, since $r = 1$ one has $\mathrm{rk}_{\mathbb{Z}_p}(\overline{A^{\Sigma}_L}) = p^2 r + 1 = p^2 + 1$ and so the last column of Table II implies that

$$\begin{aligned}p^2 + 1 = ap(p-1) + b(p-1) + c + dp + e(1 + p(p-1)) \\ + \sum_{i=0}^{p-2} f_i(p^2 - 1) + \sum_{i=0}^{p-1} g_i p^2 + \sum_{i=0}^{p-2} h_i p^2 + \sum_{i=1}^{p-2} j_i(p^2 + 1)\end{aligned}$$

Now if $f_0 > 2$ then the above equality cannot hold and so, since $f_0 > 0$ we must have $f_0 = 1$. This equality then implies that $c = 2$ and that all other coefficients are zero so that $\overline{A^{\Sigma}_L}$ is isomorphic to $\mathbb{Z}_p^2 \oplus (R_2, R_1; 1)$, as claimed.

We next use Lemma 4.2.4(i) and the second and fifth columns of Table II to compute

$$|T_{L/K}^{\Sigma}| = |\hat{H}^{-1}(G, \overline{A_L^{\Sigma}})| = |0 \oplus (\mathbb{Z}/p^2\,\mathbb{Z})| = p^2$$
$$|T_{L/F}^{\Sigma}| = |\hat{H}^{-1}(H, \overline{A_L^{\Sigma}})| = |\hat{H}^{-1}(H, \mathbb{Z}_p^2 \oplus \mathcal{O}_p \oplus \mathbb{Z}_p[H]^{p-1})| = p,$$

as needed to complete the proof. □

If we assume that $T_{L/K}^{\Sigma}$ has exponent p, then the situation becomes much more complicated. In this case the same general approach can be used to prove the following result. However, since the proof of this result is considerably more involved than that of Proposition 5.2.4, and offers no further insight into the general problem, we do not present it here.

Proposition 5.2.5. Assume that $r = 1$, that $T_{L/K}^{\Sigma}$ has exponent p, that $T_{L/K}^{\Sigma}$ does not vanish and that Leopoldt's Conjecture is valid for L at p.

Then $\overline{A_L^{\Sigma}}$ is isomorphic as a $\mathbb{Z}_p[G]$-module to either

(i) $R_2 \oplus R_1 \oplus \mathbb{Z}_p^2$, or

(ii) $(R_2, R_1; \lambda_0^i) \oplus \mathbb{Z}_p^2$ for some choice of i with $1 \le i \le p-2$, or

(iii) $(R_2, \mathbb{Z}_p \oplus E; 1 \oplus \lambda_0^i)$ for some choice of i with $1 \le i \le p-2$, or

(iv) $R_2 \oplus E \oplus \mathbb{Z}_p$, or

(v) $R_1 \oplus \mathbb{Z}_p \oplus (R_2, \mathbb{Z}_p; 1)$, or

(vi) $(R_2, E; \lambda_0^i) \oplus \mathbb{Z}_p$ for some choice of i with $1 \le i \le p-1$, or

(vii) $(R_2, \mathbb{Z}_p \oplus R_1; 1 \oplus \lambda_0^i) \oplus \mathbb{Z}_p$ for some choice of i with $0 \le i \le p-2$, or

(viii) $E \oplus (R_2, \mathbb{Z}_p; 1)$.

Remark 5.2.6. Under additional hypotheses on $|T^{\Sigma}_{L/K}|$ and $|T^{\Sigma}_{L/F}|$ our methods give a more precise version of the above result. However in no case did we find that the abstract structures of the groups $T^{\Sigma}_{L/K}$ and $T^{\Sigma}_{L/F}$ uniquely specified the isomorphism class of $\overline{A^{\Sigma}_{L}}$.

Chapter 6

Ray class groups over p-rational fields

In this chapter we investigate the Galois structure of A_L^Σ in the special case that L is a 'p-rational' field and derive consequences of our results concerning the validity (or otherwise) of Leopoldt's Conjecture at p.

6.1 Statement of the main result

Following Movahhedi and Nguyen Quang Do [32], a number field is said to be 'p-rational' if the Galois group of its maximal pro-p extension that is unramified outside p is a free pro-p group.

It is known that a number field K has this property if and only if it both validates Leopoldt's Conjecture at p and is such that A_K^p is torsion-free (see Jaulent and Nguyen Quang Do [24, Theorem 1.2]).

We further recall that any K for which both $K(\zeta_p)$ has a unique p-adic place and class number coprime to p has these properties. In particular, if p is regular, then any abelian extension of $\mathbb{Q}$ of p-power conductor is p-rational (see [24, Corollary 1.3(ii)]).

As another application of our methods, in this chapter we will prove the following result (which does not assume that G is cyclic).

In the following we write $Z(\mathcal{G})$ for the centre of a group $\mathcal{G}$.

Theorem 6.1.1. Assume that K is p-rational, let L be any finite p-power degree Galois extension of K and set $G := \mathrm{Gal}(L/K)$. Let Σ be a finite set of places of K containing all archimedean places, places above p and all those that ramify in L/K, and is also such that the group A_K^Σ is torsion-free.

Then the following claims are valid.

(i) L validates Leopoldt's Conjecture at p.

(ii) The $\mathbb{Q}_p[G]$-module spanned by B_L^Σ is free of rank r_K. The $\mathbb{Z}_p[G]$-module B_L^Σ is free if and only if one of the following conditions is satisfied:

  (a) L is contained in K^{cyc};

  (b) G is cyclic, L is disjoint from K^{cyc} and for every proper subfield F of L that contains K the maximal abelian extension of F^{cyc} in M_L^Σ is equal to M_F^Σ.

(iii) Fix a cyclic subgroup C of G and set $F := L^C$.

  (a) If γ is any element of $\mathrm{Gal}(M_L^\Sigma/F)$ of infinite order that projects to give a generator of C, then $\gamma^{|C|} \in Z(\mathrm{Gal}(M_L^\Sigma/F)) \cap A_L^\Sigma$ and the $\mathbb{Z}_p[C]$-module $A_L^\Sigma/\langle\gamma^{|C|}\rangle$ is free of rank $r_F = [G : C] \cdot r_K$.

  (b) The $\mathbb{Z}_p[C]$-module A_L^Σ is isomorphic to $\mathbb{Z}_p[C]^{[G:C]\cdot r_K} \oplus \mathbb{Z}_p$.

  (c) If $r_K = 0$, then B_L^Σ vanishes. If $r_K > 0$, then there exists an exact sequence of

$\mathbb{Z}_p[C]$-modules

$$0 \to \mathbb{Z}_p^{1-n_C} \to B_L^{\Sigma} \to \mathbb{Z}_p[C]^{[G:C]\cdot r_K} \to \mathbb{Z}_p/(\mathbb{Z}_p \cdot n_C[L : L \cap F^{\mathrm{cyc}}]) \to 0$$

where n_C is equal to 0 if $L \cap F^{\mathrm{cyc}} = F$ and equal to 1 otherwise.

Remark 6.1.2. The result of Theorem 6.1.1(i) is not new. It has been proved both by Miki [31, Theorem 3] and by Jaulent and Nguyen Quang Do [24, Corollary 1.5] via arguments using Shafarevic's description [37] of the minimal number of generators and relations of the Galois group of the maximal pro-p extension of K unramified outside Σ. If L/K is Galois of degree p it has also been proved by Miki and Sato in [31] by a method more similar to ours but still reliant on Sharaferevich's results. Finally, results of the form of Theorem 6.1.1(i) are of interest since they imply that the validity of Leopoldt's Conjecture for L at p can be deduced from its validity for the subfield K.

Remark 6.1.3. The modified ray class groups $A_L^{\Sigma}/\langle\gamma^{|C|}\rangle$ that occur in Theorem 6.1.1(iii)(a) plays a key role in the approach of Burns and Macias Castillo in [12, §5] where they are used to reinterpret the validity of Leopoldt's Conjecture at p.

6.2 Cyclic extensions of p-rational fields

As a first step in the proof of Theorem 6.1.1 we make a detailed study of the structures of ray class groups over cyclic extensions of p-rational fields.

Proposition 6.2.1. Let L/K be a cyclic extension of number fields of degree p^n and Σ a finite set of places of K containing all archimedean places, all places above p and all those that ramify in L/K. Set $G := \mathrm{Gal}(L/K)$ and fix an element γ of $\mathrm{Gal}(M_L^{\Sigma}/K)$ that has infinite order and projects to give a generator of G. For each integer i with $0 \leq i \leq n$ write L_i for the intermediate field of L/K that has degree p^i over K and γ_i for the image of γ^{p^i} in $A_{L_i}^{\Sigma}$.

If both K validates Leopoldt's Conjecture at p and the group A_K^Σ is torsion-free, then L validates Leopoldt's Conjecture at p and for each integer i the groups $A_{L_i}^\Sigma$ and $A_{L_i}^\Sigma/\langle\gamma_i\rangle$ are torsion-free.

Proof. For integers i and j with $0 \leq i < j \leq n$ we set $A_i := A_{L_i}^\Sigma$, $D_i := A_{L_i}^\Sigma/\langle\gamma_i\rangle$ and $Q_{j,i} := \mathrm{Gal}(L_j/L_i)$.

For each integer i as above we use the multiplication-by-p map on the tautological exact sequence $0 \to \langle\gamma_i\rangle \to A_i \to D_i \to 0$ to obtain an exact commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & A_i[p] \arrow[d] & D_i[p] \arrow[d] & \\
0 \arrow[r] & \langle\gamma_i\rangle \arrow[r] \arrow[d, "\times p"] & A_i \arrow[r] \arrow[d, "\times p"] & D_i \arrow[r] \arrow[d, "\times p"] & 0 \\
0 \arrow[r] & \langle\gamma_i\rangle \arrow[r] \arrow[d] & A_i \arrow[r] \arrow[d] & D_i \arrow[r] \arrow[d] & 0 \\
 & \langle\gamma_i\rangle/\langle\gamma_i^p\rangle & A_i/(A_i)^p & D_i/(D_i)^p. &
\end{tikzcd}$$

Applying the Snake Lemma to this diagram we obtain an exact sequence

$$0 \to A_i[p] \to D_i[p] \to \langle\gamma_i\rangle/\langle\gamma_i^p\rangle \xrightarrow{d_i} A_i/(A_i)^p.$$

Since the image of γ_i generates $\mathrm{Gal}(L_{i+1}/L_i)$ one has $\gamma_i \notin (A_i)^p$. Therefore the map d_i is injective and so the above sequence implies that the natural map $A_{i,[p]} \to D_{i,[p]}$ is bijective. This implies, in particular, that the group D_i is torsion-free if and only if the group A_i is torsion-free.

Until further notice, we now assume that the integer i is such that the following hypothesis is satisfied.

$(*)_i$ L_i validates Leopoldt's Conjecture at p and the group $D_i = A_i/\langle\gamma_i\rangle$ is torsion-free.

In this case, for each integer j with $i < j \leq n$ the group $H_0(Q_{j,i}, A_j)$ identifies with a subgroup of A_i and the torsion subgroup of $H_0(Q_{j,i}, D_j) = H_0(Q_{j,i}, A_j)/\langle\gamma_i^{p^{j-i}}\rangle$ is equal to

$$(A_i/\langle\gamma_i^{p^{j-i}}\rangle)_{\mathrm{tor}} \cap H_0(Q_{j,i}, A_j)/\langle\gamma_i^{p^{j-i}}\rangle = \langle\gamma_i\rangle/\langle\gamma_i^{p^{j-i}}\rangle \cap H_0(Q_{j,i}, A_j)/\langle\gamma_i^{p^{j-i}}\rangle.$$

Furthermore, this group vanishes since for any integer a with $0 \leq a < j - i$ the element $\gamma_i^{p^a}$ does not act trivially on L_j and so does not lie in $H_0(Q_{j,i}, A_j)$.

It follows that under hypothesis $(*)_i$ the group $H_0(Q_{j,i}, D_j)$ is torsion-free and hence, by the same argument as used in the proof of Lemma 4.2.4, the group $\hat{H}^{-1}(Q_{j,i}, \overline{D_j})$ vanishes.

In the case $j = i + 1$ we set $Q_i := Q_{j,i}$. Then, since Q_i has order p, there are only three isomorphism classes of indecomposable $\mathbb{Z}_p[Q_i]$-lattices, represented by $\mathbb{Z}_p, \mathbb{Z}_p[Q_i]$ and $\mathbb{Z}_p[Q_i]/(\sum_{g \in Q_i} g)$, each with the natural Q_i-action (cf. the discussion in §5.1).

We can also compute that the groups $\hat{H}^{-1}(Q_i, \mathbb{Z}_p)$ and $\hat{H}^{-1}(Q_i, \mathbb{Z}_p[Q_i])$ vanish and that the group $\hat{H}^{-1}(Q_i, \mathbb{Z}_p[Q_i]/(\sum_{g \in Q_i} g))$ has order p.

Then, since $\hat{H}^{-1}(Q_i, \overline{D_{i+1}})$ vanishes, the Krull-Schmidt theorem implies that there is an isomorphism of $\mathbb{Z}_p[Q_i]$-modules

$$\overline{D_{i+1}} \cong \mathbb{Z}_p^a \oplus \mathbb{Z}_p[Q_i]^b$$

for suitable (non-negative) integers a and b.

Now

$$\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot D_{i+1}) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot A_{i+1}) - 1 = r_{L_{i+1}} + \delta_{L_{i+1}} \geq r_{L_{i+1}} = p \cdot r_{L_i}$$

whilst, since (under hypothesis $(*)_i$) we are assuming that L_i validates Leopoldt's Conjecture at p, one also has $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot D_i) = r_{L_i}$. This gives an inequality

$$a + p \cdot b = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot D_{i+1}) \geq p \cdot r_{L_i}$$
$$= p \cdot \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot D_i) = p \cdot \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot H_0(Q_i, D_{i+1})) = p(a + b)$$

and hence implies that $a = 0$ and $b = r_{L_i}$. This shows both that L_{i+1} validates Leopoldt's Conjecture at p and also that $\overline{D_{i+1}}$ is a free $\mathbb{Z}_p[Q_i]$-module.

Then, since $\overline{D_{i+1}}$ is a free $\mathbb{Z}_p[Q_i]$-module, the tautological exact sequence

$$0 \to (D_{i+1})_{\mathrm{tor}} \to D_{i+1} \to \overline{D_{i+1}} \to 0$$

splits as a sequence of $\mathbb{Z}_p[Q_i]$-modules and so $H_0(Q_i, (D_{i+1})_{\mathrm{tor}})$ is isomorphic to a finite submodule of $H_0(Q_i, D_{i+1})$. We have already shown that the latter module is torsion-free and so $H_0(Q_i, (D_{i+1})_{\mathrm{tor}})$ vanishes. By Nakayama's Lemma, this fact then implies that $(D_{i+1})_{\mathrm{tor}}$, and hence also $(A_{i+1})_{\mathrm{tor}}$, vanishes.

At this stage we have shown that the validity of hypothesis $(*)_i$ implies the validity of hypothesis $(*)_{i+1}$.

Since the stated assumptions on $L_0 = K$ are equivalent to the validity of hypothesis $(*)_0$, induction on i shows that hypothesis $(*)_i$ is true for all integers i with $0 \leq i \leq n$ and this fact is equivalent to the claimed result. $\square$

6.3 The proof of Theorem 6.1.1

In this section we use Proposition 6.2.1 to prove Theorem 6.1.1.

As a first step we choose a finite chain of subgroups

$$\{\mathrm{id}\} = J_0 \trianglelefteq J_1 \trianglelefteq \cdots \trianglelefteq J_n = G$$

in which $|J_{i+1}/J_i| = p$ for all i with $0 \le i < n$ (this ensures that for any given intermediate field E of L/K, we have $J_i = \mathrm{Gal}(L/E)$ for some i). For each such i we set $L^i := L^{J_i}$.

Then by successively applying Proposition 6.2.1 to each of the extensions L^i/L^{i+1} for $0 \le i < n$ we deduce that L validates Leopoldt's Conjecture at p and that each group $A^{\Sigma}_{L^i}$ is torsion-free. In particular, this proves claim (i).

The first assertion of claim (ii) follows directly from combining the fact that L validates Leopoldt's Conjecture at p with Proposition 3.3.1(ii).

Since B^{Σ}_L is torsion-free (as a subgroup of A^{Σ}_L), it is a free $\mathbb{Z}_p[G]$-module if and only if it is a cohomologically trivial G-module (by [5, Chapter VI, Theorem (8.7)]). Therefore, since the above argument shows that the group $\mathrm{Gal}(M^{\Sigma}_E/L^{\mathrm{cyc}})$ is torsion-free for every intermediate field E of L/K, the second assertion of claim (ii) follows directly from Corollary 3.2.3.

We now look at claim (iii)(a). It is clear $\gamma^{|C|}$ belongs to $Z(\mathrm{Gal}(M^{\Sigma}_L/F)) \cap A^{\Sigma}_L$ and hence that the conjugation action of C on A^{Σ}_L induces an action on $D_L := A^{\Sigma}_L/\langle\gamma^{|C|}\rangle$.

We show first that D_L is a permutation module over $\mathbb{Z}_p[C]$. Since D_L is torsion-free (by Proposition 6.2.1), the observation of Remark 4.2.2 shows it is enough to prove that for each subgroup J of C the group $\hat{H}^{-1}(J, D_L)$ vanishes and we recall that the latter groups were shown to vanish in the course of proving Proposition 6.2.1.

One can check that a permutation module over $\mathbb{Z}_p[C]$ is free if and only if it spans a free $\mathbb{Q}_p[C]$-module and so claim (iii)(a) will follow if we can show that the $\mathbb{Q}_p[C]$-module $\mathbb{Q}_p \cdot D_L$ is free. To do this we note that the $\mathbb{Z}_p[C]$-module $\langle\gamma^{|C|}\rangle$ is isomorphic to $\mathbb{Z}_p$ (since C acts trivially on $\gamma^{|C|}$ which has infinite order). Then, by comparing the tautological exact sequence

$$0 \to \langle \gamma^{|C|} \rangle \to A_L^{\Sigma} \to D_L \to 0 \tag{6.1}$$

with the exact sequence (3.1), we can deduce that the $\mathbb{Q}_p[C]$-module $\mathbb{Q}_p \cdot D_L$ is isomorphic to $\mathbb{Q}_p \cdot B_L^{\Sigma}$ and hence, by Proposition 3.3.1(ii), is free, as required.

The isomorphism in claim (iii)(b) is obtained by observing that D_L is a free $\mathbb{Z}_p[C]$-module of rank $r_F = [G : C] \cdot r_K$ and hence that the exact sequence (6.1) splits.

Turning to claim (iii)(c), the first assertion is an immediate consequence of the isomorphism in (iii)(b). We therefore assume that $r_K > 0$. To derive the claimed exact sequence in this case we note first that (3.1) induces a natural exact sequence of $\mathbb{Z}_p[C]$-modules

$$0 \to \langle \gamma^{|C|} \rangle \cap B_L^{\Sigma} \to B_L^{\Sigma} \to D_L \to \Gamma_L / \langle \tilde{\gamma} \rangle \to 0 \tag{6.2}$$

where we write $\tilde{\gamma}$ for the image of $\gamma^{|C|}$ under the projection $A_L^{\Sigma} \to \Gamma_L$. Moreover, by claim (iii)(a) we know the $\mathbb{Z}_p[C]$-module D_L is free of rank $[G : C] \cdot r_K$ and it is also clear that the $\mathbb{Z}_p[C]$-module $\langle \gamma^{|C|} \rangle \cap B_L^{\Sigma}$ is either isomorphic to $\mathbb{Z}_p$ or vanishes and that the element $\tilde{\gamma}$ is correspondingly either zero or non-zero. To discuss these possibilities we set $E := L \cap F^{\mathrm{cyc}}$.

We assume first that $E = F$, and hence that L and F^{cyc} are disjoint over F. Since the $\mathbb{Z}_p$-rank of A_L^{Σ} is $|G| \cdot r_K + 1 > 1$, we can choose the element γ so that $\tilde{\gamma}$ vanishes. After choosing γ in this way, the sequence (6.2) directly gives the exact sequence in claim (iii)(c) with $n_C = 0$.

We assume next that $E \neq F$. In this case the restriction of γ to E generates the non-trivial quotient $\mathrm{Gal}(E/F)$ of Γ_F and so the restriction of γ to F^{cyc} must generate Γ_F. The image of $\tilde{\gamma}$ in Γ_F therefore generates $(\Gamma_F)^{|C|}$ and hence, since Γ_L identifies with $(\Gamma_F)^{[E:F]}$, one has $\langle \tilde{\gamma} \rangle = (\Gamma_L)^{[L:E]}$ and so the $\mathbb{Z}_p[C]$-module $\Gamma_L / \langle \tilde{\gamma} \rangle$ is isomorphic to $\mathbb{Z}_p / (\mathbb{Z}_p \cdot [L : E])$. Given these observations, the exact sequence in claim (iii)(c) (with $n_C = 1$) again follows directly from (6.2).

This completes the proof of Theorem 6.1.1.

Chapter 7

Ray class groups for abelian fields of prime power conductor

In this chapter we will always assume that p does not divide the class number of the maximal real subfield of $\mathbb{Q}(\zeta_p)$.

We recall that this condition is automatically satisfied by 'regular' primes and that Vandiver's Conjecture asserts that it is satisfied by all primes. We further recall that, by 2008, Vandiver's Conjecture had been verified for all primes up to $163,577,856$ (see Buhler and Harvey [7]).

In this chapter we combine the approach developed earlier with the known validity of the relevant case of the equivariant Tamagawa number conjecture to determine the explicit Galois structure of ray class groups over abelian extensions of $\mathbb{Q}$ that have p-power conductor.

The results that we obtain include (in Theorem 7.3.4) a natural analogue for ray class groups of Washington's determination of the explicit Galois structure of the ideal class groups of such fields [38, Theorem 10.14].

In Chapter 8 we will then use the structural results obtained here to derive some new families of congruences between the values of (suitably normalised) values at $s = 1$ of Dirichlet L-series associated to characters of p-power conductor.

7.1 General notation for cyclotomic fields

We first fix some general notation concerning cyclotomic fields.

For each natural number n we fix a primitive $p^n - th$ root of unity ζ_{p^n} in $\mathbb{Q}^c$ with the property that $\zeta_{p^n}^p = \zeta_{p^{n-1}}$ for all $n > 1$.

For each natural number n we set

$$L_n := \mathbb{Q}(\zeta_{p^n}), \quad G_n := \mathrm{Gal}(L_n/\mathbb{Q}) \ \text{ and } \ P_n := \mathrm{Gal}(L_n/L_1).$$

We also write H_n for the unique subgroup of G_n of order $p-1$ and use the restriction map $G_n \to G_1$ to identify H_n with G_1.

For each finite abelian group Γ we set $\Gamma^* := \mathrm{Hom}(\Gamma, \mathbb{Q}_p^{c\times})$ and for each ϕ in Γ^* we define an idempotent of $\mathbb{Q}_p^c[\Gamma]$ by setting

$$e_\phi := |\Gamma|^{-1} \sum_{\gamma\in\Gamma} \phi(\gamma)\gamma^{-1}.$$

We recall that, by 'orthogonality of characters' one has $e_\phi \cdot e_{\phi'} = 0$ of $\phi \neq \phi'$ and that the sum of e_ϕ over all ϕ in Γ^* is equal to $1 \in \mathbb{Z}_p[\Gamma]$.

We write $\mathbf{1}_\Gamma$ for the trivial element of Γ^* and often abbreviate the idempotent $e_{\mathbf{1}_\Gamma}$ to e_Γ.

For each element x of $\mathbb{C}_p[\Gamma]$ and each ϕ in Γ^* we write x^ϕ for the unique element of $\mathbb{C}_p$ that is defined by the equality

$$x = \sum_{\phi\in\Gamma^*} x^\phi e_\phi. \tag{7.1}$$

We use the fact that the natural direct product decomposition of abelian groups

$$G_n = P_n \times H_n$$

implies that each element θ of G_n^* can be written uniquely as a product

$$\theta = \psi \times \phi$$

(usually written as $\theta = \psi\phi$) with ψ in P_n^* and ϕ in H_n^* and also that for each ϕ in H_n^* the idempotent e_ϕ belongs to $\mathbb{Z}_p[H_n]$.

We write τ_n for the (unique) complex conjugation in H_n and define idempotents $e_+ := (1+\tau_n)/2$ and $e_- := (1-\tau_n)/2$ of $\mathbb{Z}_p[G_n]$. for any $\mathbb{Z}_p[G_n]$-module M we use submodules $M^+ := e_+(M)$ and $M^- := e_-(M)$ upon which τ_n acts as multiplication by $+1$ and -1 respectively. In particular, E^+ denotes the maximal real subfield of each subfield E of L_n. We also often use the fact that any $\mathbb{Z}_p[G_n]$-module M has a natural direct sum decomposition

$$M = M^+ \oplus M^-.$$

We write $G_n^{*,-}$ and $G_n^{*,+}$ for the subsets of G_n^* comprising characters that are odd (i.e. with $\chi(\tau_n) = -1$) and even ($\chi(\tau_n) = 1$) respectively. We define subsets $H_n^{*,+}$ and $H_n^{*,-}$ of H_n^* in a similar way and write ω for the Teichmuller character in $H_n^{*,-} = G_1^{*,-}$.

We write R_n for the ring $\mathbb{Z}_p[G_n]$ and for any homomorphism ϕ in H_n^* and any R_n-module M we set $M^\phi := e_\phi(M)$. We regard M^ϕ as a module over the ring $R_n^\phi = \mathbb{Z}_p[G_n]e_\phi$ in the natural way and note that there is a direct sum decomposition of R_n-modules

$$M = \bigoplus_{\phi \in H_n^*} M^\phi.$$

For any integer i and any $\mathbb{Z}_p[G_n]$-module M we abbreviate M^{ω^i} to $M^{(i)}$. We also write e_n for the idempotent $e_{\omega^0} = e_{H_n}$ of $\mathbb{Z}_p[H_n]$.

7.2 Torsion-free ray class groups

As in earlier sections we write A_L^p and B_L^p for the groups A_L^Σ and B_L^Σ in the case that Σ comprises all places of L that are either archimedean or p-adic.

The following result describes the explicit Galois structure of the lattices $A_{L_n}^p$ and $B_{L_n}^p$.

Theorem 7.2.1. Assume that p does not divide the class number of $\mathbb{Q}(\zeta_p)^+$. Then, for every natural number n, there are isomorphisms of $\mathbb{Z}_p[G_n]$-modules

$$A_{L_n}^p \cong B_{L_n}^p \oplus \mathbb{Z}_p \quad \text{and} \quad \overline{B_{L_n}^p} \cong \mathbb{Z}_p[G_n]^-.$$

Proof. For each natural number n we abbreviate the groups $A_{L_n}^p$ and $B_{L_n}^p$ to A_n and B_n respectively.

We recall that Brumer [6] has proved that the field L_n, and hence also L_n^+, validates Leopoldt's Conjecture at p.

The isomorphism of R_n-modules $A_n \cong B_n \oplus \mathbb{Z}_p$ is therefore a consequence of Corollary 3.2.4 with $L = L_n, K = \mathbb{Q}$ and $\Sigma = \{\infty, p\}$.

To prove that $\overline{B_n} = (\overline{B_n})^- \oplus (\overline{B_n})^+$ is a free R_n^--module we show first that $(\overline{B_n})^+$ vanishes.

To do this we observe that the maximal abelian extension of L_n^+ in $M_{L_n}^p$ is equal to $E := L_n \cdot M_{L_n^+}^p$. This implies that $A_n^+ = \mathrm{Gal}(E/L_n)$ and hence that B_n^+ is equal to $\mathrm{Gal}(E/L_n^{\mathrm{cyc}})$ which is naturally isomorphic to $\mathrm{Gal}(M_{L_n^+}^p/(L_n^+)^{\mathrm{cyc}}) = B_{L_n^+}^p$. Therefore, since L_n^+ is totally real and validates Leopoldt's Conjecture, the equality (4.1) implies that the group $(\overline{B_n})^+ = \overline{B_n^+} \cong \overline{B_{L_n^+}^p}$ vanishes, as required.

This shows that $\overline{B_n} = (\overline{B_n})^-$ and so we must now prove that $(\overline{B_n})^-$ is a free R_n^--module of rank one.

We note that $\mathbb{Z}_p \otimes_{\mathbb{Z}} W'_{L_n}$ is a free rank one R_n^--module, where W'_{L_n} is as defined just before Proposition 2.3.1. This combines with Proposition 2.3.1(iii) and (iv) and the fact that $\mathbb{Z}_p^- = 0$ to imply that for each ϕ in $H_n^{*,-}$ the $\mathbb{Z}_p$-ranks of R_n^ϕ and $(\overline{B_n})^\phi$ are equal.

Since each ring R_n^ϕ is a local ring (isomorphic to $\mathbb{Z}_p[P_n]$) it is therefore enough for to show that $\overline{B_n}$ is a free $\mathbb{Z}_p[P_n]$-module, or equivalently (by the general result [5, Chapter. VI, Theorem (8.7)]) that $\overline{B_n}$ is a cohomologically trivial P_n-module.

By the same reduction argument used in the proof of Corollary 3.2.3, it is therefore enough to prove that the Tate cohomology group $\hat{H}^{-1}(J, \overline{B_n})$ vanishes for each subgroup J of P_n and this follows directly from Lemma 7.2.3 below.

This completes the proof of Theorem 7.2.1(i). $\square$

In the following, for a number field F we use the subgroups of $F^\times$ given by

$$P_F := \{x \in F^\times : x \text{ is a } p\text{-unit}\}$$

and

$$H_F := \{x \in F^\times : F(x^{1/p})/F \text{ is unramified outside } p\}.$$

We also write Cl_F^p for the quotient of the ideal class group of F by the subgroup generated by the classes of ideals above p, and recall that $\mathrm{Cl}_F^p[p]$ denotes the subgroup of Cl_F^p consisting of elements of order p.

We use the fact that these groups are related by a natural exact sequence

$$0 \to P_F/P_F^p \to H_F(F^\times)^p/(F^\times)^p \xrightarrow{\Delta_F} \mathrm{Cl}_F^p[p] \to 0 \tag{7.2}$$

(see, for example, the proof of [1, Proposition 2.4]).

Remark 7.2.2. The map Δ_F in the sequence (7.2) can be described explicitly in the following way. If α belongs to H_F, then the fractional $\mathcal{O}_F$-ideal generated by α can be written as $\mathfrak{n}^p\mathfrak{B}$ where $\mathfrak{n}$ is a fractional ideal that is coprime to all ideals above p and $\mathfrak{B}$ is a product of prime ideals above p. Then Δ_F sends the image of α in $H_F/(F^\times)^p$ to the image of $\mathfrak{n}$ in Cl_F^p.

Lemma 7.2.3. If p does not divide $h_{\mathbb{Q}(\zeta_p)^+}$, then for each integer a with $1 \leq a \leq n$ the group $\hat{H}^{-1}(\mathrm{Gal}(L_n/L_a), \overline{B_n})$ vanishes.

Proof. If $n = 1$, this result is obvious because $\mathrm{Gal}(L_n/L_a)$ is the trivial group.

If $n > 1$, then, as already observed above, the exact sequence (3.1) splits and so Lemma 4.2.4 shows it is enough to prove $T^{\{\infty,p\}}_{L_n/L_a}$ vanishes. Recalling Lemma 4.5.4(iii), it therefore suffices to show that for any degree p Galois extension E of L_a that is not $\mathbb{Z}_p$-extendable the extension L_nE/L_a is not $\mathbb{Z}_p$-extendable.

To check this condition we use the fact that if F is either L_n or L_a and x is any element of $F^\times$, then Bertrandias and Payan [1, Proposition 2.7] have shown that $F(\sqrt[p]{x})/F$ is $\mathbb{Z}_p$-extendable if and only if x belongs to the subgroup $P_F(F^\times)^p$.

From the sequence (7.2) it is therefore enough to show that if x is any element of $L_a^\times$ with $\Delta_{L_a}(x) \neq 0$, then also $\Delta_{L_n}(x) \neq 0$.

Since there is a commutative diagram

$$\begin{tikzcd}
H_{L_n}(L_n^\times)^p/(L_n^\times)^p \arrow[r, "\Delta_{L_n}"] & \mathrm{Cl}^p_{L_n}[p] \\
H_{L_a}(L_a^\times)^p/(L_a^\times)^p \arrow[r, "\Delta_{L_a}"] \arrow[u] & \mathrm{Cl}^p_{L_a}[p] \arrow[u, "\iota_a^n"']
\end{tikzcd}$$

where the left hand vertical map is induced by the field inclusion $L_a \subseteq L_n$ and ι_n is the natural inflation, it suffices to show ι_a^n is injective.

This is true because for $b \in \{n, a\}$ one has $\mathrm{Cl}^p_{L_b}[p] = \mathrm{Cl}_{L_b}[p]$ (as all prime ideals of L_b above p are principal), because $\mathrm{Cl}^+_{L_b}[p]$ vanishes (as a consequence of the stated assumption on p) and because the inflation map $\mathrm{Cl}^-_{L_a}[p] \to \mathrm{Cl}^-_{L_n}[p]$ is injective, as is shown by Kida in [27, Proposition 1, (1.2)]. $\square$

7.3 Torsion ray class groups

In this section we state a result that determines the explicit Galois structure of the torsion subgroup of $A^p_{L_n}$ in terms of the value of Dirichlet L-series at $s = 1$ and a notion of $\mathcal{L}$-invariants.

This result is a natural analogue for ray class groups of Washington's well-known determination of the explicit Galois structure of the ideal class groups of such fields [38, Theorem 10.14].

Its proof is much more involved than that of Theorem 7.2.1, and combines the structural results established in earlier sections together with the known validity of the equivariant Tamagawa number conjecture for the pair $(h^0(\mathrm{Spec}(L_n)(1), \mathbb{Z}[G_n])$, as proved by Burns and Flach in [11].

In particular, in each of §7.3.1, §7.3.2 and §7.5 we will need to introduce notation and technical constructions that occur in the explicit form of this case of the equivariant Tamagawa number conjecture. The reader can find further details about these constructions in, for example, [3, §3 and §6.3.4] and [4, §5.3].

7.3.1 $\mathcal{L}$-invariants

We fix an isomorphism of fields j between $\mathbb{C}$ and the completion $\mathbb{C}_p$ of an algebraic closure of $\mathbb{Q}_p$ and sometimes, to reduce notation, we do not explicitly mention this isomorphism.

We set $L_{n,p} := \mathbb{Q}_p \otimes_{\mathbb{Q}} L_n$ (identified with the completion of L_n at its unique p-adic place) and recall that $(L_{n,p}^\times)_p^\wedge$ denotes the pro-p completion of $L_{n,p}^\times$.

To define $\mathcal{L}$-invariants we use the composite homomorphisms of G_n-modules

$$\log_\infty^n : \mathcal{O}_{L_n^+}^\times \to \prod_\sigma \mathbb{R}^\times \xrightarrow{(\log|\cdot|)_\sigma} \prod_\sigma \mathbb{R} = \mathbb{R} \otimes_{\mathbb{Q}} L_n^+,$$

where σ runs over the set of all embeddings $L_n^+ \to \mathbb{Q}^c$ and the first arrow is the diagonal embedding, and

$$\log_p^n : \mathcal{O}_{L_n^+}^\times \to \mathcal{O}_{L_{n,p}^+}^\times \xrightarrow{\log_p} L_{n,p}^+ = \mathbb{Q}_p \otimes_{\mathbb{Q}} L_n^+$$

where the first arrow is the obvious embedding and $\log_p$ denotes Iwasawa's p-adic logarithm.

We write $L_{n,0}^+$ for the kernel $(1-e_{G_n})L_n^+$ of the field-theoretic trace map $L_n^+ \to \mathbb{Q}$ and recall that $\mathrm{Im}(\log_\infty^n)$ is a full $\mathbb{Z}[G_n]$-lattice in $\mathbb{R} \otimes_{\mathbb{Q}} L_{n,0}^+$ and that $\mathbb{Z}_p \cdot \mathrm{Im}(\log_p^n)$ is a full $\mathbb{Z}_p[G_n]$-lattice in $\mathbb{Q}_p \otimes_{\mathbb{Q}} L_{n,0}^+$.

Hence, for any generator x of the $\mathbb{Q}[G_n]$-module spanned by $\mathcal{O}_{L_n^+}^\times$ there exists a unique element $\mathcal{L}_{\infty,p}^n(x)$ of $\mathbb{C}_p[G_n]^{+,\times}$ for which there is in $(\mathbb{C}_p \otimes_{\mathbb{Q}} L_{n,0}^+) \oplus \mathbb{C}_p\, e_{G_n}$ an equality

$$(j \otimes \mathrm{id}_{L_{n,0}^+})(\log_\infty^n(x)) + e_{G_n} = \mathcal{L}_{\infty,p}^n(x) \cdot (\log_p^n(x) + e_{G_n}). \tag{7.3}$$

Lemma 7.3.1. The element $\mathcal{L}_{\infty,p}^n(x)$ is independent of the choice of x in (7.3).

Proof. Dirichlet's regulator isomorphism implies that the $\mathbb{Q}[G_n]$-module $\mathbb{Q} \cdot \mathcal{O}_{L_n^+}^\times$ is isomorphic to $e_+ \mathbb{Q}[G_n](1 - e_{G_n})$. Therefore, if x' is any other generator of the $\mathbb{Q}[G_n]$-module spanned by $\mathcal{O}_{L_n^+}^\times$, then one has $x' = \lambda(x)$ for some element λ in $\mathbb{Q}[G_n](1 - e_{G_n})^\times$.

Then we have

$$\begin{aligned}(j\otimes \mathrm{id}_{L^+_{n,0}})(\log^n_\infty(x'))+e_{G_n} &= \lambda\cdot(j\otimes \mathrm{id}_{L^+_{n,0}})(\log^n_\infty(x))+e_{G_n}\\ &=(\lambda+e_{G_n})\cdot((j\otimes \mathrm{id}_{L^+_{n,0}})(\log^n_\infty(x))+e_{G_n})\end{aligned}$$

and

$$\begin{aligned}\log^n_p(x')+e_{G_n} &= \lambda\cdot\log^n_p(x)+e_{G_n}\\ &=(\lambda+e_{G_n})\cdot(\log^n_p(x)+e_{G_n}).\end{aligned}$$

Since $\lambda+e_{G_n}\in\mathbb{Q}[G_n]^\times$ this shows that the element $\mathcal{L}^n_{\infty,p}$ does not depend on x. □

Definition 7.3.2. In view of Lemma 7.3.1 we can write $\mathcal{L}^n_{\infty,p}$ instead of $\mathcal{L}^n_{\infty,p}(x)$ and we refer to this element as the '$\mathcal{L}$-invariant' associated to L_n.

For each character ψ in G_n^* we abbreviate the ψ-component $\mathcal{L}^{n,\psi}_{\infty,p}$ of $\mathcal{L}^n_{\infty,p}$ (as defined via the decomposition (7.1)) to $\mathcal{L}^\psi_{\infty,p}$.

7.3.2 Statement of the main result

In order to state the main result of this section we fix a topological generator $\gamma_\mathbb{Q}$ of $\Gamma_\mathbb{Q}$.

Noting that G_n/H_n can be identified with the (unique) quotient of $\Gamma_\mathbb{Q}$ of order p^{n-1} we also fix a generating element γ_n of G_n that projects to the same element of G_n/H_n as $\gamma_\mathbb{Q}$.

We write $\chi_\mathbb{Q}$ for the cyclotomic character of $\Gamma_\mathbb{Q}$ and define an element

$$\epsilon^n_{\gamma_\mathbb{Q}}:=\sum_{\psi\in G_n^*}\epsilon^\psi_{\gamma_\mathbb{Q}}e_\psi$$

of $\mathbb{Q}_p[G_n]^\times$ by setting for each ψ in G_n^*

$$\epsilon_{\gamma_{\mathbb{Q}}}^{\psi} := \begin{cases} \log_p(\chi_{\mathbb{Q}}(\gamma_{\mathbb{Q}}))^{-1}, & \text{if } \psi = \mathbf{1}_{G_n}, \\ (1-\psi(\gamma_n))^{-1}, & \text{if } \psi(H_n) = 1 \text{ and } \psi(\gamma_n) \neq 1, \\ 1, & \text{if } \psi(H_n) \neq 1. \end{cases}$$

Finally we set

$$\theta_n^*(1) := (1-p^{-1})e_{\mathbf{1}_{G_n}} + \sum_{\psi \in G_n^* \setminus \{\mathbf{1}_{G_n}\}} L(\psi,1) \cdot e_\psi \in \mathbb{C}_p[G_n]^\times$$

where $L(\psi,1)$ is the value at $z=1$ of the Dirichlet L-series $\sum_{n\geq 1} \frac{\psi(n)}{n^z}$.

Remark 7.3.3. The element $\theta_n^*(1)$ is most naturally interpreted as the leading term at $z=1$ of the p-truncated equivariant Dedekind zeta function of $L_n/\mathbb{Q}$ that is discussed by Breuning and Burns in [4].

Theorem 7.3.4. Assume that p does not divide $h_{\mathbb{Q}(\zeta_p)^+}$. Then for every natural number n the groups $A^p_{L_n,\mathrm{tor}}$ and $B^{p,+}_{L_n}$ coincide, one has

$$\theta_n^*(1) \cdot \epsilon^n_{\gamma_{\mathbb{Q}}} \mathcal{L}^n_{\infty,p} \in \mathbb{Z}_p[G_n]^+ \cap (\mathbb{C}_p[G_n]^+)^\times$$

and there is an isomorphism of $\mathbb{Z}_p[G_n]$-modules of the form

$$A^p_{L_n,\mathrm{tor}} \cong \mathbb{Z}_p[G_n]^+/(\theta_n^*(1) \cdot \epsilon^n_{\gamma_{\mathbb{Q}}} \mathcal{L}^n_{\infty,p}).$$

The proof of this result will occupy the next three sections.

7.4 The key exact triangle

In this section we fix Σ to be $\{\infty, p\}$ and we adapt a construction of Burns and Macias Castillo from [12] to refine the explicit description of $R\Gamma_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma}, \mathbb{Z}_p(1))$ that is given in Proposition 2.3.1. In particular, we will construct an exact triangle in $D^{\text{perf}}(R_n)$ that plays an important part in the proof of Theorem 7.3.4.

To do this we fix an element γ of $\text{Gal}(M^p_{L_n}/\mathbb{Q})$ that projects to give both the element γ_n of G_n and the element $\gamma_{\mathbb{Q}}$ of $\Gamma_{\mathbb{Q}}$ that are fixed at the beginning of §7.3.2 (this is possible since the actions of γ_n and $\gamma_{\mathbb{Q}}$ are chosen to agree on $L_n \cap \mathbb{Q}^{\text{cyc}}$).

We then write $C^\bullet_{n,\gamma}$ for the complex of projective R_n-modules

$$R_n^{(0)} \xrightarrow{d_\gamma} R_n^{(0)} \tag{7.4}$$

where the first term is placed in degree two and d_γ satisfies $d_\gamma(e_n) = (1-\gamma_n)e_n$.

We identify the groups $H^2(C^\bullet_{n,\gamma}) = \ker(d_\gamma)$ and $H^3(C^\bullet_{n,\gamma}) = \text{cok}(d_\gamma)$ with $\mathbb{Z}_p$ via the maps of R_n-modules $\iota : \mathbb{Z}_p \to R_n^{(0)}$ and $\epsilon : R_n^{(0)} \to \mathbb{Z}_p$ with $\iota(1) = \sum_{g \in P_n} ge_n$ and $\epsilon(ge_n) = 1$ for all $g \in G_n$.

Finally we set $W_{n,p} := W_{L_n,p} (= \mathbb{Z}_p \otimes_{\mathbb{Z}} W'_{L_n})$ and write $C^\bullet_n$ for the complex

$$W_{n,p} \xrightarrow{0} R_n^- \tag{7.5}$$

where the first term is placed in degree one.

In the following result we use the fact that $\overline{B_n}$ is a free rank one R_n^--module (by Theorem 7.2.1). We also use the general notation of Example 2.2.1.

Proposition 7.4.1. Assume that p does not divide $h_{\mathbb{Q}(\zeta_p)^+}$ and fix an element b of $B_n^- = A_n^-$ that projects to give a basis of the R_n^--module $\overline{B_n}$. Then there exists a canonical exact triangle in $D^{\mathrm{perf}}(R_n)$ of the form

$$C^\bullet_{n,\gamma} \oplus C^\bullet_n \xrightarrow{\theta_\gamma \oplus \theta_b} R\Gamma_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma}, \mathbb{Z}_p(1)) \to A_{n,\mathrm{tor}}[-2] \to (C^\bullet_{n,\gamma} \oplus C^\bullet_b)[1] \tag{7.6}$$

in which $H^2(\theta_\gamma)(1) = \gamma^{|G_n|} \in A_n$, $H^3(\theta_\gamma)$ is the identity on $\mathbb{Z}_p$, $H^1(\theta_b)$ is the canonical identification $W_{n,p} = H^1_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma}, \mathbb{Z}_p(1))$ (coming from Proposition 3.3.1(i) and the known validity of Leopoldt's Conjecture for L_n at p) and $H^2(\theta_b)$ sends each element x of $\mathbb{Z}_p[G_n]^-$ to $x(b)$.

Before proving this result we state an interesting consequence concerning Galois structures.

Corollary 7.4.2. The G_n-module $A_{n,\mathrm{tor}}$ is cohomologically trivial.

Proof. The exact triangle (7.6) shows that the complex $A_{n,\mathrm{tor}}[-2]$ belongs to $D^{\mathrm{perf}}(\mathbb{Z}_p[G_n])$.

Since $A_{n,\mathrm{tor}}$ is finite, and $H^i(A_{n,\mathrm{tor}}[-2])$ is equal to $A_{n,\mathrm{tor}}$ if $i = 2$ and to zero if $i \neq 2$, Lemma 2.2.3 implies that $A_{n,\mathrm{tor}}$ is a cohomologically trivial G_n-module. □

In the rest of this section we prove Proposition 7.4.1.

We set $E^\bullet_n := R\Gamma_{c,\text{ét}}(\mathcal{O}_{L_n,\Sigma}, \mathbb{Z}_p(1))$ and recall from Proposition 2.3.1(i) that $E^\bullet_n$ belongs to $D^{\mathrm{perf}}(R_n)$.

It is also clear from the definition (7.4) that $C^\bullet_{n,\gamma}$ belongs to $D^{\mathrm{perf}}(R_n)$ and, since $W_{n,p}$ is a free R_n^--module of rank one (as already used in the proof of Theorem 7.2.1), the definition (7.5) makes clear that $C^\bullet_n$ belongs to $D^{\mathrm{perf}}(R_n)$.

Now, since each term of $C^\bullet_n$ is a finitely generated projective R_n-module and each differential is zero, one knows that the homomorphism

$$\mathrm{Hom}_{D(R_n)}(C^\bullet_n, E^\bullet_n) \to \mathrm{Hom}_{R_n}(W_{n,p}, H^1(E^\bullet_n)) \oplus \mathrm{Hom}_{R_n}(R_n^-, H^2(E^\bullet_n))$$

sending each φ to $(H^1(\varphi), H^2(\varphi))$ is bijective.

From the explicit descriptions of the cohomology of $E_n^\bullet$ given in Proposition 2.3.1(iii), it follows that there exists a unique morphism $\theta_b : C_n^\bullet \to E_n^\bullet$ in $D(R_n)$ with the given descriptions of $H^1(\theta_b)$ and $H^2(\theta_b)$.

The construction of a morphism $\theta_\gamma : C_{n,\gamma}^\bullet \to E_n^\bullet$ in $D^{\mathrm{perf}}(R_n)$ with the given descriptions of $H^2(\theta_\gamma)$ and $H^3(\theta_\gamma)$ is much more involved but is fortunately described by Burns and Macias Castillo in [12, Proposition 4.3].

Writing $D_n^\bullet$ for the mapping cone of $\theta_\gamma \oplus \theta_b$ we obtain an exact triangle of the form

$$C_{n,\gamma}^\bullet \oplus C_n^\bullet \xrightarrow{\theta_\gamma \oplus \theta_b} E_n^\bullet \xrightarrow{\psi} \mathrm{Cone}(\theta_\gamma \oplus \theta_b) \to$$

and so it is enough to show that the long exact cohomology sequence of this triangle implies that $\mathrm{Cone}(\theta_\gamma \oplus \theta_b)$ is acyclic outside degree two and such that $H^2(D_n^\bullet)$ is isomorphic as an R_n-module to $A_{n,\mathrm{tor}}$.

Now the long exact cohomology sequence has the form

$$\begin{aligned}
\ldots \to H^0(C_{n,\gamma}^\bullet \oplus C_n^\bullet) &\xrightarrow{H^0(\theta_\gamma \oplus \theta_b)} H^0(E_n^\bullet) \xrightarrow{H^0(\psi)} H^0(D_n^\bullet) \\
\xrightarrow{d_{0,1}} H^1(C_{n,\gamma}^\bullet \oplus C_n^\bullet) &\xrightarrow{H^1(\theta_\gamma \oplus \theta_b)} H^1(E_n^\bullet) \xrightarrow{H^1(\psi)} H^1(D_n^\bullet) \\
\xrightarrow{d_{1,2}} H^2(C_{n,\gamma}^\bullet \oplus C_n^\bullet) &\xrightarrow{H^2(\theta_\gamma \oplus \theta_b)} H^2(E_n^\bullet) \xrightarrow{H^2(\psi)} H^2(D_n^\bullet) \\
\xrightarrow{d_{2,3}} H^3(C_{n,\gamma}^\bullet \oplus C_n^\bullet) &\xrightarrow{H^3(\theta_\gamma \oplus \theta_b)} H^3(E_n^\bullet) \xrightarrow{H^3(\psi)} H^3(D_n^\bullet) \\
\xrightarrow{d_{3,4}} H^4(C_{n,\gamma}^\bullet \oplus C_n^\bullet) &\xrightarrow{H^4(\theta_\gamma \oplus \theta_b)} H^4(E_n^\bullet) \xrightarrow{H^4(\psi)} H^4(D_n^\bullet) \to \ldots
\end{aligned}$$

and so combines with the descriptions (7.4), (7.5) and Proposition 2.3.1(ii) to make clear that $H^i(D_n^\bullet)$ vanishes for $i \notin \{0,1,2,3\}$.

The exact sequence also shows that the (obvious) injectivity of $H^1(\theta_b)$ implies that $H^0(D_n^\bullet)$ vanishes, that the surjectivity of $H^3(\theta_\gamma)$ implies that $H^3(D_n^\bullet)$ vanishes, that the (obvious) surjectivity of $H^1(\theta_b)$ and injectivity of both $H^2(\theta_\gamma)$ and $H^2(\theta_b)$ combine imply $H^1(D_n^\bullet)$

vanishes and that the (obvious) injectivity of $H^3(\theta_\gamma)$ gives rise to a short exact sequence

$$0 \to \mathrm{Im}(H^2(\theta_\gamma \oplus \theta_b)) \to A_n \to H^2(D_n^\bullet) \to 0. \tag{7.7}$$

Now, since the exact sequence (3.1) splits in this case we have $A_{n,\mathrm{tor}} = B_{n,\mathrm{tor}}$. In addition, the group

$$\mathrm{Im}(H^2(\theta_\gamma \oplus \theta_b)) = \mathrm{Im}(H^2(\theta_\gamma)) + \mathrm{Im}(H^2(\theta_b))$$

is torsion-free and so disjoint from $A_{n,\mathrm{tor}}$. Hence, since $H^2(\theta_\gamma)(1) = \gamma^{|G_n|}$ is a topological generator of Γ_{L_n} and our choice of the element b implies that $B_{n,\mathrm{tor}} + \mathrm{Im}(H^2(\theta_b)) = B_n$, we therefore obtain a direct sum decomposition of R_n-modules

$$A_n = A_{n,\mathrm{tor}} \oplus \mathrm{Im}(H^2(\theta_\gamma \oplus \theta_b)).$$

Given this decomposition, we find that the exact sequence (7.7) induces an isomorphism of R_n-modules $H^2(D_n^\bullet) \cong A_{n,\mathrm{tor}}$, as required.

This completes the proof of Proposition 7.4.1.

7.5 Logarithmic resolvents, $\mathcal{L}$-invariants and Fitting ideals

7.5.1 Statement of the main result

Recall that we have fixed an isomorphism of fields $j : \mathbb{C} \cong \mathbb{C}_p$.

We also now fix an embedding $\sigma_n : L_n \to \mathbb{Q}^c$ and then for any element u of $(L_{n,p}^\times)_p^\wedge$ and any character χ in $G_n^{*,-}$ we set

$$\mathcal{LR}_u^\chi := \frac{1}{j(2\pi i)} \sum_{g \in G_n} \chi(g)^{-1} \log_p(\sigma_n(g(u))) \in \mathbb{C}_p\,.$$

Definition 7.5.1. The *normalised logarithmic resolvent* of an element u of $(L_{n,p}^{\times})_p^{\wedge}$ is the element of $\mathbb{C}_p[G_n]$ given by

$$\mathcal{LR}_u := \sum_{\chi \in G_n^{*,-}} \mathcal{LR}_u^{\chi} \cdot e_{\chi}.$$

In this section we will combine the exact triangle constructed in Proposition 7.4.1 together with the validity of the equivariant Tamagawa number conjecture for $h^0(\mathrm{Spec}(L_n)(1), \mathbb{Z}[G_n])$ to prove the following result.

Theorem 7.5.2. Fix an element u of $(L_{n,p}^{\times,-})_p^{\wedge}$ that the global reciprocity map $(L_{n,p}^{\times})_p^{\wedge} \to A_n$ sends to a generator of the (cyclic) R_n^--module $\overline{B_n}$.

Then the element $\theta_n^*(1)(\mathcal{LR}_u + \epsilon_{\gamma_{\mathbb{Q}}}^n \mathcal{L}_{\infty,p}^n)$ belongs to R_n and generates $\mathrm{Fit}_{R_n}(A_{n,\mathrm{tor}})$.

Remark 7.5.3. Since $\mathcal{LR}_u$ belongs to $\mathbb{C}_p[G_n]^-$ and $\mathcal{L}_{\infty,p}^n$ to $\mathbb{C}_p[G_n]^+$ Theorem 7.5.2 is true if and only one has both

$$(\theta_n^*(1) \cdot \mathcal{LR}_u) \cdot R_n^- = \mathrm{Fit}_{R_n^-}(A_{n,\mathrm{tor}}^-) \tag{7.8}$$

and

$$(\theta_n^*(1)\epsilon_{\gamma_{\mathbb{Q}}}^n \mathcal{L}_{\infty,p}^n) \cdot R_n^+ = \mathrm{Fit}_{R_n^+}(A_{n,\mathrm{tor}}^+). \tag{7.9}$$

In the next two subsections we shall consider these equalities separately.

7.5.2 The minus component

We write Λ_n for the semisimple $\mathbb{C}_p$-algebra $\mathbb{C}_p \cdot R_n = \mathbb{C}_p[G_n]$.

To prove (7.8) we adapt an argument of Castillo and Jones from [13]. Specifically, we use the fact that the proof of [13, Proposition 2.2] (which depends on the known validity of the relevant case of the equivariant Tamagawa number conjecture) describes an explicit isomorphism of Λ_n-modules $\Phi_n : \mathbb{C}_p \cdot H^2(E_n^{\bullet})^- \cong \mathbb{C}_p \cdot H^1(E_n^{\bullet})^-$ for which there is an equality of graded invertible R_n^--modules

$$(\theta_n^*(1)\cdot R_n^-,0)=\vartheta_{\Phi_n^{-1}}(\mathrm{Det}_{R_n^-}(E_n^{\bullet,-}))^{-1} \tag{7.10}$$

where here we have used the general notation of §2.2.3.

To describe the isomorphism Φ_n we write ϵ_u for the homomorphism of R_n-modules $H^1(E_n^\bullet)=W_{n,p}\to H^2(E_n^\bullet)$ that sends the R_n-generator

$$w_n := 2\pi i\cdot(\sigma_n-\sigma_n\circ\tau_n)$$

of $W_{n,p}$ to the image of the chosen element u under the reciprocity map $(L_{n,p}^{\times,-})_p^\wedge\to B_n^-=A_n^-=H^2(E_n^\bullet)^-$.

Then our explicit definition of the logarithmic resolvent $\mathcal{LR}_u$ is chosen so that by working through the maps that are used (in the proof of [13, Proposition 2.2]) to define Φ_n one finds that

$$(\Phi_n\circ(\mathbb{C}_p\otimes_{\mathbb{Z}_p}\epsilon_u))(w_n)=\mathcal{LR}_u\cdot w_n$$

and hence that

$$\det_{\Lambda_n}(\Phi_n\circ(\mathbb{C}_p\otimes_{\mathbb{Z}_p}\epsilon_u))=\mathcal{LR}_u.$$

In particular, since our choice of u implies that the map $\mathbb{C}_p\otimes\epsilon_u$ is invertible, this equality combines with (7.10) to give an equality

$$((\theta_n^*(1)\cdot\mathcal{LR}_u)R_n^-,0)=\vartheta_{\mathbb{C}_p\otimes\epsilon_u}(\mathrm{Det}_{R_n^-}(E_n^{\bullet,-}))^{-1}. \tag{7.11}$$

To compute the right hand side of this equality we use the exact triangle constructed in Proposition 7.4.1 in the case that the element b is chosen to have the same image in $\overline{B_n}$ as the image of our chosen element u under the reciprocity map.

In this case the image of $H^2(\theta_b)(e_-)$ in $\overline{B_n}$ is equal to the image of $H^1(\theta_b)(w_n)$ under $\mathbb{C}_p \otimes \epsilon_u$ and so, writing μ_b for the isomorphism of (free rank one) R_n^--modules $W_{n,p} \to R_n^-$ that sends w_n to $(1-\tau_n)/2$, we can compute that

$$\begin{aligned}\vartheta_{\mathbb{C}_p \otimes \epsilon_u}(\mathrm{Det}_{R_n^-}(E_n^{\bullet,-})) =& \vartheta_{\mathbb{C}_p \otimes \mu_b}(\mathrm{Det}_{R_n^-}(C_n^{\bullet})) \otimes \mathrm{Det}_{R_n^-}(A_{n,\mathrm{tor}}^-[-2]) \\ =& \mathrm{Det}_{R_n^-}(A_{n,\mathrm{tor}}^-[-2]) \\ =& (\mathrm{Fit}_{R_n^-}(A_{n,\mathrm{tor}}^-)^{-1}, 0).\end{aligned} \tag{7.12}$$

Here, the first equality is obtained by applying the general result of (2.7) to the exact triangle obtained by applying e_- to the triangle in Proposition 7.4.1 and noting that all terms of the complex $C_{n,\gamma}^{\bullet,-}$ are zero, and the third equality is a particular case of Remark 2.2.6.

Also the second equality in (7.12) is true because we have

$$\begin{aligned}\vartheta_{\mathbb{C}_p \otimes \mu_b}(\mathrm{Det}_{R_n^-}(C_n^{\bullet})) &= (\vartheta_{\mathrm{ev}} \circ (\mathrm{Det}_R(\mu_b)^{-1} \otimes \mathrm{id}))((\mathrm{Hom}_{R_n^-}(W_{n,p}, R_n^-), -1) \otimes (R_n^-, 1)) \\ &= \vartheta_{\mathrm{ev}}((\mathrm{Hom}_{R_n^-}(R_n^-, R_n^-), -1) \otimes (R_n^-, 1)) \\ &= (R_n^-, 0)\end{aligned}$$

where ϑ_{ev} is the evaluation pairing on R_n^- (in the sense of (2.4)) and the second equality is true because $\mu_b(W_{n,p}) = R_n^-$.

By combining the equalities (7.11) and (7.12) we deduce that $(\theta_n^*(1) \cdot \mathcal{LR}_u)R_n^-$ is equal to $\mathrm{Fit}_{R_n^-}(A_{n,\mathrm{tor}}^-)$, as required to prove (7.8).

7.5.3 The plus component

In this section we prove the equality (7.9), and therefore complete the proof of Theorem 7.5.2. We continue to write Λ_n for $\mathbb{C}_p \cdot R_n = \mathbb{C}_p[G_n]$.

The homomorphisms $\log_\infty^n$ and $\log_p^n$ that are described in §7.3.1 combine to give an isomorphism of $\mathbb{C}_p[G_n]$-modules

$$\log_{\infty,p}^n : \mathbb{C}_p \otimes_{\mathbb{Q}} L_{n,0}^+ \xrightarrow{(\mathbb{C}_p \cdot \log_\infty^n)^{-1}} \mathbb{C}_p \otimes_{\mathbb{Z}} \mathcal{O}_{L_n^+}^\times \xrightarrow{\mathbb{C}_p \cdot \log_p^n} \mathbb{C}_p \otimes_{\mathbb{Q}} L_{n,0}^+,$$

and that, by the very definition (in Definition 7.3.2) of the $\mathcal{L}$-invariant $\mathcal{L}_{\infty,p}^n$, one has

$$\mathcal{L}_{\infty,p}^n = \det_{\Lambda_n}(\log_{\infty,p}^n). \tag{7.13}$$

We also have that, since $W_{L_n,p}^+ = 0$, Proposition 3.3.1(i) implies that $H^a(E_n^{\bullet,+})$ is non-zero for only $a = 2$ and $a = 3$, and also that $B_{L_n}^{p,+}$ is finite so that we have a composite isomorphism of $\mathbb{Q}_p[G_n]$-modules

$$\kappa_n : \mathbb{Q}_p \cdot H^2(E_n^{\bullet,+}) = \mathbb{Q}_p \cdot \Gamma_{L_n^+} \xrightarrow{\log_p \circ \chi_{\mathbb{Q}}} \mathbb{Q}_p = \mathbb{Q}_p \cdot H^3(E_n^{\bullet,+}).$$

We recall that, in terms of these maps, the (known) validity of the equivariant Tamagawa number conjecture for $(h^0(\mathrm{Spec}(L_n^+))(1), \mathbb{Z}[G_n]^+)$ implies that

$$(\theta_n^*(1)\mathcal{L}_{\infty,p}^n \cdot R_n^+, 0) = \vartheta_{\Xi_n}(\mathrm{Det}_{R_n^+}(E_n^{\bullet,+}))^{-1}. \tag{7.14}$$

In fact this equivalence is proved directly by the explicit computation of Breuning and Burns in [4, §5.3], after taking into account (7.13) and the well-known fact that the isomorphism $\mathbb{Q}_p \cdot \mathbb{Z}_p^\times \cong \mathbb{Q}_p \cdot \Gamma_{\mathbb{Q}}$ that is induced by the global reciprocity map is the inverse of the isomorphism $\mathbb{Q}_p \cdot \Gamma_{\mathbb{Q}} \cong \mathbb{Q}_p \cdot \mathbb{Z}_p^\times$ that is induced by $\chi_{\mathbb{Q}}$.

We next apply the general result of (2.7) to the exact triangle obtained by applying e_+ to the triangle in Proposition 7.4.1 to see that there is an equality

$$\vartheta_{\Xi_n}(\mathrm{Det}_{R_n^+}(E_n^{\bullet,+})) = \vartheta_{\Xi_n^\gamma}(\mathrm{Det}_{R_n^+}(C_{n,\gamma}^\bullet)) \otimes \mathrm{Det}_{R_n^+}(A_{n,\mathrm{tor}}^+[-2]) \tag{7.15}$$

with Ξ_n^γ the composite isomorphism of $\mathbb{Q}_p[G_n]$-modules

$$\mathbb{Q}_p \cdot H^2(C_{n,\gamma}^\bullet) \xrightarrow{\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2(\theta_\gamma)} \mathbb{Q}_p \cdot H^2(E_n^{\bullet,+}) \xrightarrow{\Xi_n} \mathbb{Q}_p \cdot H^3(E_n^{\bullet,+}) = \mathbb{Q}_p \cdot H^3(C_{n,\gamma}^\bullet).$$

It is now enough to show that

$$\vartheta_{\Xi_n^\gamma}(\mathrm{Det}_{R_n}(C_{n,\gamma}^\bullet)) = ((\epsilon_{\gamma_\mathbb{Q}}^n)^{-1} R_n^+, 0), \tag{7.16}$$

since, if this is true, then it can be combined with (7.14) and (7.15) to directly give the required equality

$$(\theta_n^*(1)\epsilon_{\gamma_\mathbb{Q}}^n \mathcal{L}_{\infty,p}^n \cdot R_n^+, 0) = \mathrm{Det}_{R_n^+}(A_{n,\mathrm{tor}}^+[-2])^{-1} = (\mathrm{Fit}_{R_n^+}(A_{n,\mathrm{tor}}^+), 0),$$

where the last equality follows by another application of Remark 2.2.6.

We prove the necessary equality (7.16) after multiplying by the idempotent e_{ω^a} for every even integer a with $0 \le a \le p-2$.

In fact, if $a \neq 0$, then $C_{n,\gamma}^{\bullet,(a)}$ is the zero complex and the explicit definition of $\epsilon_{\gamma_\mathbb{Q}}^n$ gives

$$e_{\omega^a}\epsilon_{\gamma_\mathbb{Q}}^n = \epsilon_{\gamma_\mathbb{Q}}^{\omega^a} e_{\omega^a} = e_{\omega^a}$$

and so this component of (7.16) is true.

To compute $\vartheta_{\Xi_n^\gamma}(\mathrm{Det}_{R_n}(C_{n,\gamma}^\bullet))^{(0)}$ we note that the explicit definition of $\mathrm{Det}_{R_n^{(0)}}(C_{n,\gamma}^{\bullet,(0)})$ (as recalled in §2.2.3) shows that

$$\mathrm{Det}_{R_n^{(0)}}(C_{n,\gamma}^{\bullet,(0)}) = (R_n^{(0)} \cdot x, 0)$$

with $x := (e_n, 1) \otimes (e_n^*, -1)$ where e_n^* is the dual of e_n in $\mathrm{Hom}_{R_n^{(0)}}(R_n^{(0)}, R_n^{(0)})$.

We now use the fact that

$$e_n = e_{G_n} + (e_n - e_{G_n}),$$

$$\mathbb{Q}_p \cdot H^2(C_{n,\gamma}^{\bullet}) = \mathbb{Q}_p \cdot e_{G_n},$$

$$d_\gamma(e_n - e_{G_n}) = (1 - \gamma_n)e_n$$

and

$$\Xi_n^\gamma(e_{G_n}) = \log_p(\chi_{\mathbb{Q}}(\gamma)) = \log_p(\chi_{\mathbb{Q}}(\gamma_{\mathbb{Q}}))$$

to compute that

$$\begin{aligned}
\vartheta_{\Xi_n^\gamma}(x) &= ((1 - \gamma_n)e_n, 0) + (\vartheta'_{\mathrm{ev}} \circ (\mathrm{Det}_{\mathbb{Q}_p \cdot R_n^+}(\Xi_n^\gamma) \otimes \mathrm{id}))((e_{G_n}, 1) \otimes (e_{G_n}^*, -1))) \\
&= ((1 - \gamma_n)e_n, 0) + \vartheta'_{\mathrm{ev}}((\log_p(\chi_{\mathbb{Q}}(\gamma_{\mathbb{Q}}))e_{G_n}, 1) \otimes (e_{G_n}^*, -1)) \\
&= ((1 - \gamma_n)e_n + \log_p(\chi_{\mathbb{Q}}(\gamma_{\mathbb{Q}}))e_{G_n}, 0) \\
&= (e_n(\epsilon_{\gamma_{\mathbb{Q}}}^n)^{-1}, 0).
\end{aligned}$$

Here ϑ'_{ev} is the map induced by the evaluation pairing on $\mathbb{Q}_p \cdot e_{G_n}$, $e_{G_n}^*$ denotes the dual of e_{G_n} in $\mathrm{Hom}_{\mathbb{Q}_p}(\mathbb{Q}_p \cdot e_{G_n}, \mathbb{Q}_p)$ and the last equality is a direct consequence of the explicit definition of $\epsilon_{\gamma_{\mathbb{Q}}}^n$.

This concludes the proof of the equality (7.16) and hence also the proof of Theorem 7.5.2.

7.6 Bernoulli numbers and the proof of Theorem 7.3.4

The result of Proposition 7.6.3 below implies that the group $B^-_{n,\mathrm{tor}} = A^-_{n,\mathrm{tor}}$ vanishes and that the R_n-module $A_{n,\mathrm{tor}} = B^+_{n,\mathrm{tor}} = B^+_n$ is cyclic.

The last fact combines with the general property recalled in Remark 2.2.7 and the result of Theorem 7.5.2 to imply that

$$\mathrm{Ann}_{R_n^+}(A^+_{n,\mathrm{tor}}) = \mathrm{Fit}_{R_n^+}(A^+_{n,\mathrm{tor}}) = (\theta^*_n(1)(\mathcal{LR}_\pi + \epsilon^n_{\gamma_\mathbb{Q}}\mathcal{L}^n_{\infty,p}))\cdot R_n^+ = (\theta^*_n(1)\epsilon^n_{\gamma_\mathbb{Q}}\mathcal{L}^n_{\infty,p})\cdot R_n^+$$

and hence gives an isomorphism of R_n-modules

$$A_{n,\mathrm{tor}} = A^+_{n,\mathrm{tor}} \cong R_n^+/(\theta^*_n(1)\cdot\epsilon^n_{\gamma_\mathbb{Q}}\mathcal{L}^n_{\infty,p}).$$

This completes the proof of Theorem 7.3.4.

Before stating the next result we recall an important definition.

Definition 7.6.1. If χ is a Dirichlet character of conductor N, then the *generalised Bernoulli number* of χ are the coefficients $B_{n,\chi}$ that appear in the power series expansion

$$\sum_{a=1}^{N}\frac{\chi(a)te^{at}}{e^{Nt}-1} = \sum_{n\geq 0} B_{n,\chi}\frac{t^n}{n!}.$$

Example 7.6.2. If χ is the trivial character, then $B_{1,\chi} = \frac{1}{2}$ and if χ is any non-trivial even character (so that $\chi(-1) = 1$), then $B_{1,\chi} = 0$ (for details see [38, §4]).

Proposition 7.6.3. Assume that p does not divide $h_{\mathbb{Q}(\zeta_p)^+}$ and fix an integer i with $0 \leq i \leq p-2$.

(i) The group $B^{(i)}_{n,\mathrm{tor}} = A^{(i)}_{n,\mathrm{tor}}$ vanishes if either i is odd or if both i is even and the Bernoulli number $B_{1,\omega^{i-1}}$ is not divisible by p.

(ii) In all cases the group $B^{(i)}_{n,\mathrm{tor}} = A^{(i)}_{n,\mathrm{tor}}$ is a cyclic $R^{(i)}_n$-module.

Proof. Lemma 3.3.2(iii) implies that there is an isomorphism of $R^{(i)}_1$-modules between $H_0(P_n, B^{(i)}_n)$ and $B^{(i)}_1$. Since the $R^{(i)}_n$-module $\overline{B^{(i)}_n}$ is projective (by Theorem 7.2.1) this isomorphism restricts to give an isomorphism of finite groups

$$H_0(P_n, A^{(i)}_{n,\mathrm{tor}}) = H_0(P_n, B^{(i)}_{n,\mathrm{tor}}) \cong B^{(i)}_{1,\mathrm{tor}} = A^{(i)}_{1,\mathrm{tor}}. \tag{7.17}$$

We now write I_{P_n} for the augmentation ideal of the group ring $\mathbb{Z}_p[P_n]$. Then the Jacobson radical $\mathrm{Jac}(R^{(i)}_n)$ of $R^{(i)}_n$ is equal to $p \cdot R^{(i)}_n + I_{P_n} \cdot R^{(i)}_n$ and the quotient ring $R^{(i)}_n/\mathrm{Jac}(R^{(i)}_n)$ identifies with $\mathbb{F}_p$.

Since (7.17) induces an isomorphism of $\mathbb{F}_p$-modules

$$A^{(i)}_{n,\mathrm{tor}}/(\mathrm{Jac}(R^{(i)}_n) \cdot A^{(i)}_{n,\mathrm{tor}}) \cong A^{(i)}_{1,\mathrm{tor}}/p$$

Nakayama's Lemma implies that the minimal number of generators of the $R^{(i)}_n$-module $A^{(i)}_{n,\mathrm{tor}}$ is equal to $\dim_{\mathbb{F}_p}(A^{(i)}_{1,\mathrm{tor}}/p)$ and so we now compute this dimension.

We claim that

$$\begin{aligned}
\dim_{\mathbb{F}_p}(A^{(i)}_{1,\mathrm{tor}}/p) &= \dim_{\mathbb{F}_p}(A^{(i)}_1/p) - \dim_{\mathbb{F}_p}(\overline{A^{(i)}_1}/p) \\
&= \dim_{\mathbb{F}_p}((H_{L_1}/(L_1^\times)^p)^{(1-i)}) - \dim_{\mathbb{F}_p}(\overline{B^{(i)}_1}/p) - \dim_{\mathbb{F}_p}(\mathbb{Z}^{(i)}_p/p) \\
&= \dim_{\mathbb{F}_p}((P_{L_1}/P^p_{L_1})^{(1-i)}) + \dim_{\mathbb{F}_p}(\mathrm{Cl}^p_{L_1}[p]^{(1-i)}) \\
&\qquad\qquad - \dim_{\mathbb{F}_p}(\overline{B^{(i)}_1}/p) - \dim_{\mathbb{F}_p}(\mathbb{Z}^{(i)}_p/p) \\
&= \dim_{\mathbb{F}_p}(\langle \zeta_p \rangle^{(1-i)}) + \dim_{\mathbb{F}_p}((\mathcal{O}^\times_{L_1^+}/(\mathcal{O}_{L_1^+})^p)^{(1-i)}) + \dim_{\mathbb{F}_p}((\mathbb{Z}/p)^{(1-i)}) \\
&\quad + \dim_{\mathbb{F}_p}((\mathrm{Cl}_{L_1}/p)^{(1-i)}) - \dim_{\mathbb{F}_p}(\overline{B^{(i)}_1}/p) - \dim_{\mathbb{F}_p}(\mathbb{Z}^{(i)}_p/p).
\end{aligned} \tag{7.18}$$

The first equality in (7.18) is obvious and the second is true since Kummer theory combines with the definition of H_{L_1} (just prior to (7.2)) to give an isomorphism of $\mathbb{Z}_p[G_1]$-modules

$$A_1/p \cong \mathrm{Hom}(H_{L_1}(L_1^\times)^p/(L_1^\times)^p, \langle\zeta_p\rangle)$$

and because the exact sequence of $\mathbb{Z}_p[G_1]$-modules $0 \to B_1 \to A_1 \to \Gamma_{L_1} \to 0$ splits (as the order of G_1 is prime to p).

The third equality in (7.18) is obtained by multiplying the exact sequence (7.2) by $e_{\omega^{1-i}}$.

The last equality in (7.18) is obtained by combined the following three facts: the unique prime ideal of L_1 above p is principal so $\mathrm{Cl}_{L_1}^p = \mathrm{Cl}_{L_1}$ and for any finite $\mathbb{Z}_p[G_1]$-module M the modules $M[p]$ and M/p are isomorphic; for the same reason there is an exact sequence of G_1-modules $0 \to \mathcal{O}_{L_1}^\times \to P_{L_1} \to \mathbb{Z} \to 0$ (where the third arrow sends each element of P_{L_1} to its valuation at the unique place of L_1 above p); finally, one has $\mathcal{O}_{L_1}^\times = \mathcal{O}_{L_1^+}^\times \cdot \langle\zeta_p\rangle$ (by Washington [38, Proposition 1.5]) and so there is a direct sum decomposition of $\mathbb{F}_p[G_1]$-modules $\mathcal{O}_{L_1}^\times/(\mathcal{O}_{L_1}^\times)^p = \mathcal{O}_{L_1^+}^\times/(\mathcal{O}_{L_1^+}^\times)^p \oplus \langle\zeta_p\rangle$.

To compute the last expression in (7.18) we combine the following:

- $\dim_{\mathbb{F}_p}(\langle\zeta_p\rangle^{(1-i)})$ and $\dim_{\mathbb{F}_p}(\mathbb{Z}_p^{(i)}/p)$ are both equal to 1 if $i = 0$ and to 0 otherwise.
- From [38, Proposition 8.13] one knows that $\dim_{\mathbb{F}_p}((\mathcal{O}_{L_1^+}^\times/(\mathcal{O}_{L_1^+}^\times)^p)^{(1-i)})$ is equal to 1 if i is both odd and bigger than 1 and is equal to zero otherwise.
- $\dim_{\mathbb{F}_p}((\mathbb{Z}_p/p)^{(1-i)})$ is equal to 1 if $i = 1$ and to 0 otherwise.
- From [38, Corollary 10.15] one knows that $\dim_{\mathbb{F}_p}(\mathrm{Cl}_{L_1}^{(1-i)}/p)$ is equal to 1 if i is even and such that $B_{1,\omega^{i-1}}$ is divisible by p and is equal to 0 otherwise.
- Theorem 7.2.1 implies that $\dim_{\mathbb{F}_p}(\overline{B_1^{(i)}}/p)$ is equal to 1 if i is odd and is equal to 0 otherwise.

After summarising these results in the following table

	$i=0$	$i=1$	i even, $i>0$	i odd, $i>1$
$\langle\zeta_p\rangle^{(1-i)}$	1	0	0	0
$(\mathcal{O}_{L_1^+}/(\mathcal{O}_{L_1^+})^p)^{(1-i)}$	0	0	0	1
$(\mathbb{Z}_p/p)^{(1-i)}$	0	1	0	0
$\mathrm{Cl}_{L_1}^{(1-i)}/p$	$\begin{cases} 1 & \text{if } p \mid B_{1,\omega^{-1}} \\ 0 & \text{otherwise} \end{cases}$	0	$\begin{cases} 1 & \text{if } p \mid B_{1,\omega^{i-1}} \\ 0 & \text{otherwise} \end{cases}$	0
$\overline{B_1^{(i)}}/p$	0	1	0	1
$\mathbb{Z}_p^{(i)}/p$	1	0	0	0

one checks that (7.18) implies that

$$\dim_{\mathbb{F}_p}(A_{1,\mathrm{tor}}^{(i)}/p) = \begin{cases} 1, & \text{if } i \text{ is even and } p \text{ divides } B_{1,\omega^{i-1}}, \\ 0, & \text{otherwise.} \end{cases}$$

This proves both claims (i) and (ii). $\square$

Chapter 8

L-value congruences for characters of prime power conductor

In this chapter we derive from the main results in Chapter 7 an apparently new family of congruence relations between the values at $z = 1$ of Dirichlet L-series of characters of prime power conductor.

8.1 Statement of the main result

In the following result we use the $\mathcal{L}$-invariant introduced in Definition 7.3.2, the logarithmic resolvent introduced in Definition 7.5.1 and the explicit elements $\epsilon^{\chi}_{\gamma_{\mathbb{Q}}}$ of $\mathbb{Q}_p[G_n]^{\times}$ introduced at the beginning of §7.3.2.

We also use the same notation regarding elements of $\mathbb{Q}_p[G_n]$ as described in (7.1).

Theorem 8.1.1. Assume that p does not divide the class number of $\mathbb{Q}(\zeta_p)^+$. Then the following claims are valid for every natural number n.

(i) Fix an even integer i with $0 \le i \le p-3$ and for each ψ in P_n^* set

$$L^*(\psi\omega^i, 1) := \begin{cases} 1 - p^{-1}, & \text{if } \psi = \mathbf{1}_{P_n} \text{ and } i = 0, \\ L(\psi\omega^i, 1), & \text{otherwise.} \end{cases}$$

(a) If p divides the generalised Bernoulli number $B_{1,\omega^{i-1}}$, then $A^{p,(i)}_{L_n,\mathrm{tor}}$ has order at least p^n and the product $\epsilon^{\omega^i}_{\gamma_{\mathbb{Q}}} \cdot \mathcal{L}^{\omega^i}_{\infty,p} \cdot L^*(\omega^i, 1)$ belongs to $p \cdot \mathbb{Z}_p$.

(b) If p does not divide $B_{1,\omega^{i-1}}$, then $A^{p,(i)}_{L_n,\mathrm{tor}}$ is trivial and the product $\epsilon^{\omega^i}_{\gamma_{\mathbb{Q}}} \cdot \mathcal{L}^{\omega^i}_{\infty,p} \cdot L^*(\omega^i, 1)$ belongs to $\mathbb{Z}_p^\times$.

(c) In all cases, for every element g in G_n the congruence

$$\sum_{\psi \in P_n^*} (\psi\omega^i)(g) \cdot \epsilon^{\psi\omega^i}_{\gamma_{\mathbb{Q}}} \cdot \mathcal{L}^{\psi\omega^i}_{\infty,p} \cdot L^*(\psi\omega^i, 1) \equiv 0 \pmod{|G| \cdot \mathbb{Z}_p}$$

is valid in $\mathbb{C}_p$.

(ii) Fix an element u of $(\mathbb{Z}_p \hat{\otimes} L^\times_{n,p})^-$ that the global reciprocity map of L_n sends to a generator of the (cyclic) $\mathbb{Z}_p[G_n]$-module $\overline{B^p_{L_n}}$. Then for every odd integer i with $1 \le i \le p-2$ the product $\mathcal{LR}^{\omega^i}_u \cdot L(\omega^i, 1)$ belongs to $\mathbb{Z}_p^\times$ and for every element g of G_n the congruence

$$\sum_{\psi \in P_n^*} (\psi\omega^i)(g) \cdot \mathcal{LR}^{\psi\omega^i}_u \cdot L(\psi\omega^i, 1) \equiv 0 \pmod{|G| \cdot \mathbb{Z}_p}$$

is valid in $\mathbb{C}_p$.

8.2 The proof of Theorem 8.1.1

We first consider Theorem 8.1.1(i) and so fix an even integer i with $0 \le i \le p-3$.

To prove the first assertion of claim (i)(a) we assume that p divides $B_{1,\omega^{i-1}}$. In this case

Proposition 7.6.3 implies that $A^{(i)}_{1,\mathrm{tor}} \neq 0$ and then the surjection (7.17) implies that $A^{(i)}_{n,\mathrm{tor}} \neq 0$.

Since Corollary 7.4.2 implies that $A^{(i)}_{n,\mathrm{tor}}$ is a cohomologically trivial P_n-module we can therefore apply Lemma 2.2.4 to deduce that $|A^{(i)}_{n,\mathrm{tor}}|$ is at least $p^{\Delta_{P_n}}$ and since one has $\Delta_{P_n} = n$ (as P_n is cyclic of order p^{n-1}) this proves the first assertion of claim (i)(a).

The first assertion of claim (i)(b) follows immediately from Proposition 7.6.3.

To prove all remaining assertions of Theorem 8.1.1(i) we note that Proposition 7.6.3 combines with the displayed isomorphism in Theorem 7.3.4 to imply that $e_{(i)}\theta_n^*(1)\cdot\epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p}$ belongs to $R_n^{(i)\times}$ if p does not divide $B_{1,\omega^{i-1}}$ and to $R_n^{(i)} \setminus R_n^{(i)\times}$ if p divides $B_{1,\omega^{i-1}}$.

We also recall that $R_n^{(i)}$ is isomorphic to the ring $\mathbb{Z}_p[P_n]$ and that for each ψ in P_n^* one has

$$(e_{(i)}\theta_n^*(1)\cdot\epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p})^{\psi} = \epsilon^{\psi\omega^i}_{\gamma_{\mathbb{Q}}}\mathcal{L}^{\psi\omega^i}_{\infty,p}\cdot L^*(\psi\omega^i,1).$$

Given these facts, all remaining assertions of Theorem 8.1.1(i) can be obtained by applying the following result with $\Gamma = P_n$ and $x = e_{(i)}\theta_n^*(1)\cdot\epsilon^n_{\gamma_{\mathbb{Q}}}\mathcal{L}^n_{\infty,p}$.

Lemma 8.2.1. Let Γ be a finite abelian p-group and fix x in $\mathbb{C}_p[\Gamma]$.

(i) x belongs to $\mathbb{Z}_p[\Gamma]$ if and only if for every element γ of Γ the congruence

$$\sum_{\psi\in\Gamma^*}\psi(\gamma)x^{\psi} \equiv 0 \pmod{|\Gamma|\cdot\mathbb{Z}_p}$$

is valid in $\mathbb{C}_p$.

(ii) If x belongs to $\mathbb{Z}_p[\Gamma]$, then x belongs to $\mathbb{Z}_p[\Gamma]\setminus\mathbb{Z}_p[\Gamma]^{\times}$, resp. to $\mathbb{Z}_p[\Gamma]^{\times}$, if and only if $x^{\mathbf{1}_\Gamma}$ belongs to $p\cdot\mathbb{Z}_p$, resp. to $\mathbb{Z}_p^{\times}$.

Proof. To prove claim (i), we have

$$x = \sum_{\psi\in\Gamma^*}x^{\psi}e_{\psi} = \sum_{\psi\in\Gamma^*}x^{\psi}|\Gamma|^{-1}\sum_{\gamma\in\Gamma}\psi(\gamma)\gamma^{-1} = \sum_{\gamma\in\Gamma}|\Gamma|^{-1}(\sum_{\psi\in\Gamma^*}\psi(\gamma)x^{\psi})\gamma^{-1}$$

and hence x belongs to $\mathbb{Z}_p[\Gamma]$ if and only if for every element γ of Γ the sum $\sum_{\psi\in\Gamma^*}\psi(\gamma)x^\psi$ belongs to $|\Gamma|\cdot\mathbb{Z}_p$.

Next, we note that $\mathbb{Z}_p[\Gamma]$ is a local ring with maximal ideal equal to the set of elements $x=\sum_{\gamma\in\Gamma}x_\gamma\gamma$, with each x_γ in $\mathbb{Z}_p$, such that $\sum_{\gamma\in\Gamma}x_\gamma$ belongs to $p\cdot\mathbb{Z}_p$. This implies claim (ii) because

$$\sum_{\gamma\in\Gamma}x_\gamma=\sum_{\gamma\in\Gamma}\sum_{\psi\in\Gamma^*}|\Gamma|^{-1}\psi(\gamma)x^\psi=\sum_{\psi\in\Gamma^*}|\Gamma|^{-1}(\sum_{\gamma\in\Gamma}\psi(\gamma))x^\psi=x^{\mathbf{1}_\Gamma}.$$

□

To prove Theorem 8.1.1(ii) we now fix an odd integer i with $1\le i\le p-3$.

In this case Proposition 7.6.3 implies that $A_{n,\mathrm{tor}}^{(i)}$ vanishes. This implies that $\mathrm{Fit}_{R_n}(A_{n,\mathrm{tor}})^{(i)}$ $=\mathrm{Fit}_{R_n^{(i)}}(A_{n,\mathrm{tor}}^{(i)})$ is equal to $R_n^{(i)}$ and hence, via the result of Theorem 7.5.2, that the element

$$e_{(i)}\theta_n^*(1)(\mathcal{L}\mathcal{R}_u+\epsilon_{\gamma_\mathbb{Q}}^n\mathcal{L}_{\infty,p}^n)=e_{(i)}\theta_n^*(1)\cdot\mathcal{L}\mathcal{R}_u$$

is a unit of the ring $R_n^{(i)}$.

This fact implies Theorem 8.1.1(ii) via a simple application of Lemma 8.2.1 (in just the same way that it was used to prove the second assertion of Theorem 8.1.1(i)(b) and the corresponding case of the congruences in Theorem 8.1.1(i)(c)).

This completes the proof of Theorem 8.1.1.

Bibliography

[1] F. Bertrandias, J.-J Payan, *Γ-extensions et invariants cyclotomiques*, Ann. Sci. Éc. Norm. Su. **5** (1972) 517-543.

[2] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, in The Grothendieck Festschrift Vol I, Progress in Math. Vol 86, Birkhäuser (1990), 333-400.

[3] M. Breuning, D. Burns, *Leading Terms of Artin L-Functions at* $s = 0$ *and* $s = 1$, Compositio Mathematica 143 (2007), 1427-1464.

[4] M. Breuning, D. Burns, *On equivariant Dedekind Zeta-functions at* $s = 1$, Documenta Math., Extra Volume: Andrei A. Suslin's Sixtieth Birthday, 119-146 (2010).

[5] K. S. Brown, *Cohomology of Groups*, Graduate Texts in Mathematics **87**, Springer, New York (1992).

[6] A. Brumer, *On the units of algebraic number fields*, Mathematics **14** (1967) 121-124.

[7] J. P. Buhler, D. Harvey, *Irregular primes to* 163 *million*, Math. Comp. **80** (2011) 2435-2444.

[8] D. Burns, *Leading terms and values of equivariant motivic L-functions*, Pure App. Math. Q. (2010) **6** 83-172 (John Tate Special Issue, Part II).

[9] D. Burns, *On the Galois structure of arithmetic cohomology III: Selmer groups of critical motives*, to appear in Kyoto J. Math.

[10] D. Burns, M. Flach, *Equivariant Tamagawa numbers for motives with (non-commutative) coefficients*, Doc. Math. **6** (2001) 501-570.

[11] D. Burns, M. Flach, *On the equivariant Tamagawa number conjecture for Tate motives II*, Documenta Math. Extra Volume: John H. Coates Sixtieth Birthday, 133-163.

[12] D. Burns, D. Macias Castillo, *On p-adic L-series, p-adic cohomology and class field theory*, to appear in J. reine u. angew. Math.

[13] H. Castillo, A. Jones, *On the values of Dedekind Zeta functions at* $s = 1$ *and annihilation of class groups*, Acta Arith. **160** (2013) 67-93.

[14] C. W. Curtis, I. Reiner *Methods of Representation Theory, Volume I*, John Wiley and Sons, New York, 1987.

[15] F. E. Diederichsen, *Über die Ausreduktion ganzahliger Gruppendarstellungen bei arithmetischer Aquivalenz*, Abh. Math. Sem. Univ. Hamburg **14** (1940) 357-412.

[16] G. G. Elder, M. L. Madan, *Galois module structure of the integers in wildly ramified cyclic extensions*, J. Number Theor. **47** (1994) 138-174.

[17] G. G. Elder, M. L. Madan, *Galois module structure of the ring of integers in wildly ramified* $C_p \times C_p$ *extensions*, Canad. J. Math. **49** (1997) 722-735.

[18] M. Flach, *Euler characteristics in relative K-groups*, Bull. London Math. Soc. **32** (2000) 272-284.

[19] G. Gras, *Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'um corps de nombres*, J. reine u. angew. Math. **333** (1982) 86-132.

[20] A. Heller, I. Reiner, *Representations of cyclic groups in rings of integers, I*, Ann. Math. **77** (1963) 318-328.

[21] A. Heller, I. Reiner, *Representations of cyclic groups in rings of integers. II,* Ann. Math. **76** (1962) 73-92.

[22] D. Hemard, *Modules galoisiennes de torsion et plongements dans les $\mathbb{Z}_p$-extensions*, J. Number Theory **30** (1988) 357-374.

[23] P. J. Hilton, U. Stammbach, *A course in homological algebra*, Graduate Texts in Mathematics **4**, Springer-Verlag (1997).

[24] J-F. Jaulent, T. Nguyen Quang Do, *Corps p-rationnels, corps p-réguliers et ramification restreinte*, J. Th. Nombres Bordeaux **5** (1993) 343-363.

[25] K. Kato, *Lectures on the approach to Iwasawa theory of Hasse-Weil L-functions via B_{dR}, Part I,* In: Arithmetical Algebraic Geometry (ed. E. Ballico), Lecture Notes in Math. 1553 (1993) 50-163, Springer, New York, 1993.

[26] C. Khare, J-P. Wintenberger, *Ramifications in Iwasawa Theory and Splitting Conjectures*, Int. Math. Res. Notices **2014**, 1 (2014) 194-223.

[27] Y. Kida, *l-Extensions of CM-Fields and Cyclotomic invariants*, J. Number Theory **12** (1980) 519-528.

[28] F. Knudsen, D. Mumford, *The projectivity of the moduli space of stable curves I: Preliminaries on 'det' and 'Div'*, Math. Scand. **39** (1976) 19-55.

[29] T.-Y. Lam. *A first course in noncommutative rings*, Graduate Texts in Mathematics **131**, Springer-Verlag (1991).

[30] D. Macias Castillo, *On the Krull-Schmidt decomposition of Mordell-Weil groups*, to appear in Tokyo J. Math.

[31] H. Miki, H. Sato, *Leopoldt's conjecture and Reiner's theorem*, J. Math. Soc. Japan **36** (1984) 47-52.

[32] A. Movahhedi, T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Sém. Th. Nombres Paris 1987/1988, Prog. in Math. **89** (1990) 155-200.

[33] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Springer-Verlag, Berlin (2000).

[34] D. G. Northcott, *Finite Free Resolutions*, Cambridge University Press (1976).

[35] M. Rzedowski-Calderón, G. D. Villa Salvador, M. L. Madan, *Galois module structure of rings of integers*, Math. Z. **204** (1990) 401-424.

[36] S. Seo, *On first layers of $\mathbb{Z}_p$-extensions*, J. Number Theory, **133** (2013) 4010-4023.

[37] I. R. Shafarevic, *Extensions with prescribed ramification points*, Publ. Math. I.H.E.S. **36** (1986) 71-95.

[38] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer-Verlag (1997).

[39] A. V. Yakovlev, *Homological definability of p-adic representations of a ring with power basis*, Izvestia A N SSSR, ser. Math. **34** (1970) 321-342 (Russian).

[40] A. V. Yakovlev, *Homological definability of p-adic representations of groups with cyclic Sylow p-subgroup*, An. St. Univ. Ovidius Constanţa **4** (1996) 206-221.